Cisco ASA 5500 Series Adaptive Security Appliance Getting Started Guide

For the Cisco ASA 5510, ASA 5520, and ASA 5540

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

Customer Order Number: DOC-7817611=
Text Part Number: 78-17611-01

Cisco ASA 5500 Series Adaptive Security Appliance Getting Started Guide

CONTENTS

Before You Begin

Use the following table to find the installation and configuration steps that are required for your implementation of the adaptive security appliance.

The adaptive security appliance implementations included in this document are as follows:

ASA 5500

To Do This ...	See ...
Install the chassis	Chapter 2, “Installing the Cisco ASA 5500”
Connect interface cables	Chapter 4, “Connecting Interface Cables”
Perform initial setup of the adaptive security appliance	Chapter 5, “Configuring the Adaptive Security Appliance”

To Do This ... (continued)	See ...
Configure the adaptive security appliance for your implementation	Chapter 6, "Scenario: DMZ Configuration" Chapter 7, "Scenario: Remote-Access VPN Configuration" Chapter 8, "Scenario: Site-to-Site VPN Configuration"
Configure optional and advanced features	*Cisco Security Appliance Command Line Configuration Guide*
Operate the system on a daily basis	*Cisco Security Appliance Command Reference* *Cisco Security Appliance Logging Configuration and System Log Messages*

ASA 5500 with AIP SSM

To Do This	See ....
Install the chassis	Chapter 2, "Installing the Cisco ASA 5500"
Install the AIP SSM	Chapter 3, "Installing Optional SSMs"
Connect interface cables	Chapter 4, "Connecting Interface Cables"
Perform initial setup the adaptive security appliance	Chapter 5, "Configuring the Adaptive Security Appliance"
Configure the adaptive security appliance for AIP SSM	Chapter 9, "Configuring the AIP SSM"

To Do This .... (continued)	See ....
Configure IPS software for intrusion prevention	*Configuring the Cisco Intrusion Prevention System Sensor Using the Command Line Interface* *Cisco Intrusion Prevention System Command Reference*
Refine configuration and configure optional and advanced features	*Cisco Security Appliance Command Line Configuration Guide* *Cisco Security Appliance Command Reference* *Cisco Security Appliance Logging Configuration and System Log Messages*

ASA 5500 with CSC SSM

To Do This	To Do This ....
Install the chassis	Chapter 2, "Installing the Cisco ASA 5500"
Install the CSC SSM	Chapter 3, "Installing Optional SSMs"
Connect interface cables	Chapter 4, "Connecting Interface Cables"
Perform initial setup of the adaptive security appliance	Chapter 5, "Configuring the Adaptive Security Appliance"
Configure the adaptive security appliance for content security	Chapter 10, "Configuring the CSC SSM"

To Do This .... (continued)	To Do This ....
Configure the CSC SSM	*Cisco Content Security and Control SSM Administrator Guide*
Refine configuration and configure optional and advanced features	*Cisco Security Appliance Command Line Configuration Guide* *Cisco Security Appliance Command Reference* *Cisco Security Appliance Logging Configuration and System Log Messages*

ASA 5500 with 4GE SSM

To Do This ...	See ...
Install the chassis	Chapter 2, "Installing the Cisco ASA 5500"
Install the 4GE SSM	Chapter 3, "Installing Optional SSMs"
Connect interface cables	Chapter 4, "Connecting Interface Cables"
Perform initial setup of the adaptive security appliance	Chapter 5, "Configuring the Adaptive Security Appliance"
Install the fiber optic module	Chapter 3, "Installing Optional SSMs"
Refine configuration and configure optional and advanced features	*Cisco Security Appliance Command Line Configuration Guide* *Cisco Security Appliance Command Reference* *Cisco Security Appliance Logging Configuration and System Log Messages*

Installing the Cisco ASA 5500

Warning **Only trained and qualified personnel should be allowed to install, replace, or service this equipment.**

Caution Read the safety warnings in the *Regulatory Compliance and Safety Information for the Cisco ASA 5500 Series* and follow proper safety procedures when performing these steps.

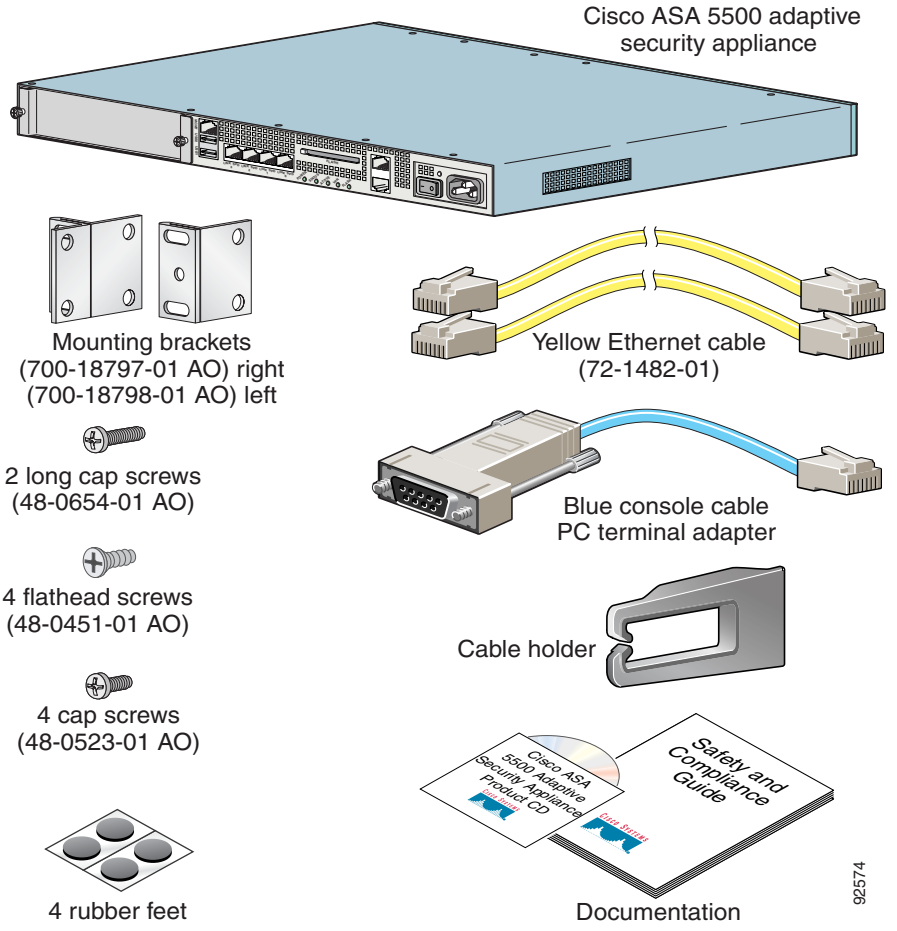
This chapter describes the product overview, memory requirements and rack-mount and installation procedures for the adaptive security appliance. This chapter includes the following sections:

Note The illustrations in this document show the Cisco ASA 5540 adaptive security appliance. The Cisco ASA 5510 adaptive security appliance and Cisco ASA 5520 adaptive security appliance are identical, containing the same back panel features and indicators.

Verifying the Package Contents

Verify the contents of the packing box to ensure that you have received all items necessary to install your Cisco ASA 5500 series adaptive security appliance. See Figure 2-1.

Figure 2-1 Contents of ASA 5500 Package



Installing the Chassis

This section describes how to rack-mount and install the adaptive security appliance. You can mount the adaptive security appliance in a 19-inch rack (with a 17.5- or 17.75-inch opening).

Warning **To prevent bodily injury when mounting or servicing this unit in a rack, you must take special precautions to ensure that the system remains stable. The following guidelines are provided to ensure your safety.**

The following information can help plan equipment rack installation:

- Allow clearance around the rack for maintenance.
- When mounting a device in an enclosed rack ensure adequate ventilation. An enclosed rack should never be overcrowded. Make sure that the rack is not congested, because each unit generates heat.
- When mounting a device in an open rack, make sure that the rack frame does not block the intake or exhaust ports.
- If the rack contains only one unit, mount the unit at the bottom of the rack.
- If the rack is partially filled, load the rack from the bottom to the top, with the heaviest component at the bottom of the rack.
- If the rack contains stabilizing devices, install the stabilizers prior to mounting or servicing the unit in the rack.

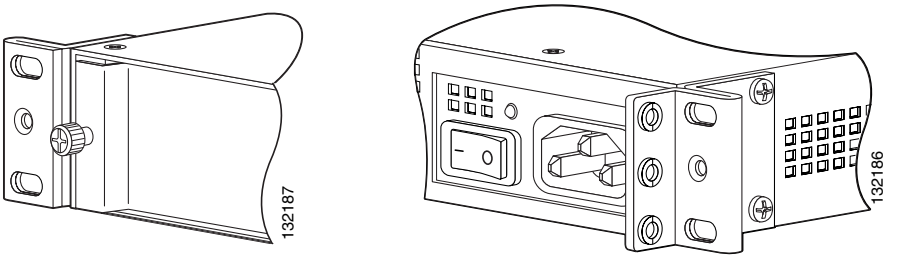
Warning **Before performing any of the following procedures, ensure that power is removed from the DC circuit. To ensure that all power is OFF, locate the circuit breaker on the panel board that services the DC circuit, switch the circuit breaker to the OFF position, and tape the switch handle of the circuit breaker in the OFF position.**

Rack-Mounting the Chassis

To rack-mount the chassis, perform the following steps:

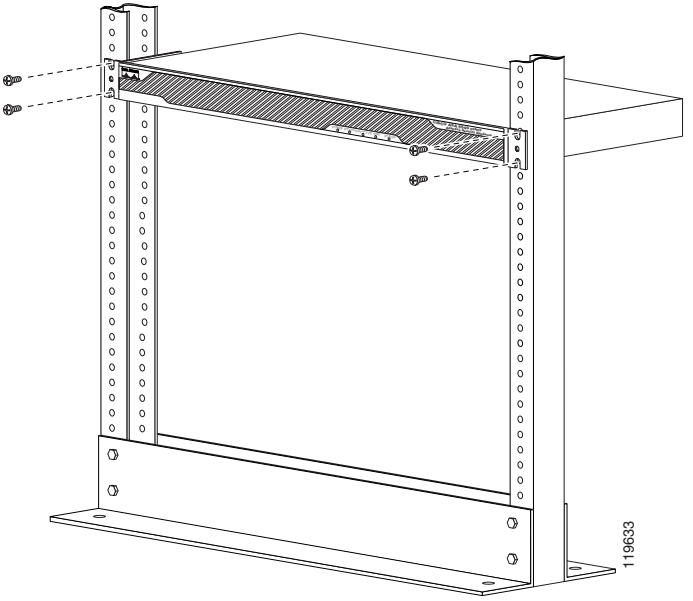
Step 1 Attach the rack-mount brackets to the chassis using the supplied screws. Attach the brackets to the holes as shown in Figure 2-2. After the brackets are secured to the chassis, you can rack-mount it.

Figure 2-2 Installing the Right and Left Brackets



Step 2 Attach the chassis to the rack using the supplied screws, as shown in Figure 2-3.

Figure 2-3 Rack-Mounting the Chassis

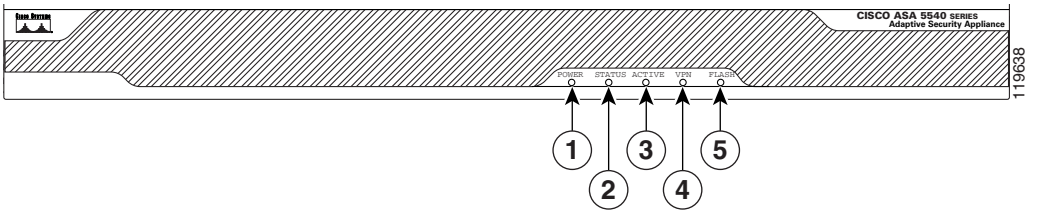


To remove the chassis from the rack, remove the screws that attach the chassis to the rack, and then remove the chassis.

Ports and LEDs

This section describes the front and rear panels. Figure 2-4 shows the front panel LEDs.

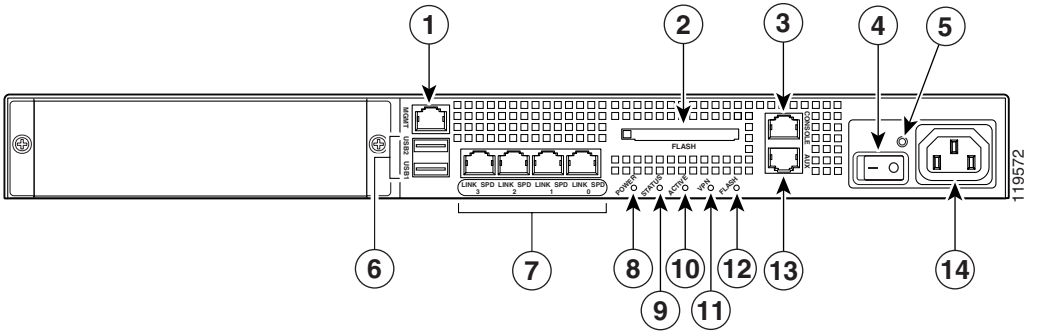
Figure 2-4 Front Panel LEDs



	LED	Color	State	Description
1	Power	Green	On	The system has power.
2	Status	Green	Flashing	The power-up diagnostics are running or the system is booting.
			Solid	The system has passed power-up diagnostics.
		Amber	Solid	The power-up diagnostics have failed.
3	Active	Green	Solid	This is the active failover device.
		Amber	Solid	This is the standby failover device.
4	VPN	Green	Solid	VPN tunnel is established.
5	Flash	Green	Solid	The CompactFlash is being accessed.

Figure 2-5 shows the rear panel features for the adaptive security appliance.

Figure 2-5 Rear Panel LEDs and Ports (AC Power Supply Model Shown)



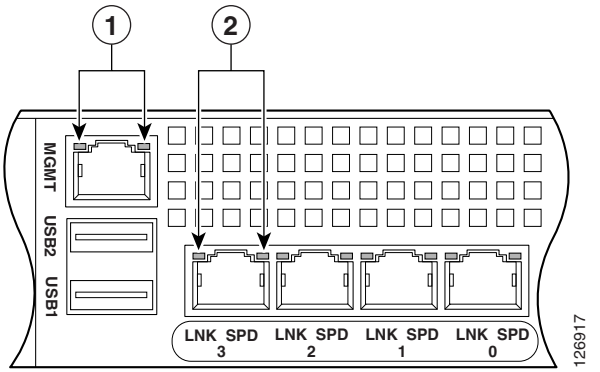
1	Management Port[1]	**6**	USB 2.0 interfaces[2]	**11**	VPN LED
2	External CompactFlash slot	**7**	Network interfaces[3]	**12**	Flash LED
3	Serial Console port	**8**	Power indicator LED	**13**	AUX port
4	Power switch	**9**	Status indicator LED	**14**	Power connector
5	Power indicator LED	**10**	Active LED		

1. The management 0/0 interface is a Fast Ethernet interface designed for management traffic only.
2. Not supported at this time.
3. GigabiteEthernet interfaces, from right to left, GigabitEthernet 0/0, GigabitEthernet 0/1, GigabitEthernet 0/2, and GigabitEthernet 0/3.

For more information on the Management Port, see the "Management-Only" section in the *Cisco Security Appliance Command Reference.*

Figure 2-6 shows the adaptive security appliance rear panel LEDs.

Figure 2-6 Rear Panel Link and Speed Indicator LEDs



1	MGMT indicator LEDs	**2**	Network interface LEDs

Table 2-1 lists the rear MGMT and Network interface LEDs.

Table 2-1 Link and Speed LEDs

Indicator	Color	Description
Left side	Solid green	Physical link
	Green flashing	Network activity
Right side	Not lit	10 Mbps
	Green	100 Mbps
	Amber	1000 Mbps

Note The ASA 5510 adaptive security appliance only supports 10/100BaseTX. The ASA 5520 adaptive security appliance and the ASA 5540 adaptive security appliance support 1000BaseT.

What to Do Next

Continue with one of the following chapters:

To Do This ...	See ...
Install SSMs you purchased but that have not yet been installed	Chapter 3, "Installing Optional SSMs"
Continue with connecting interface cables	Chapter 4, "Connecting Interface Cables"

Installing Optional SSMs

This chapter provides information about installing optional SSMs (Security Services Modules) and their components. You only need to use the procedures in this chapter if you purchased an optional SSM but it is not yet installed.

This chapter includes the following sections:

Cisco 4GE SSM

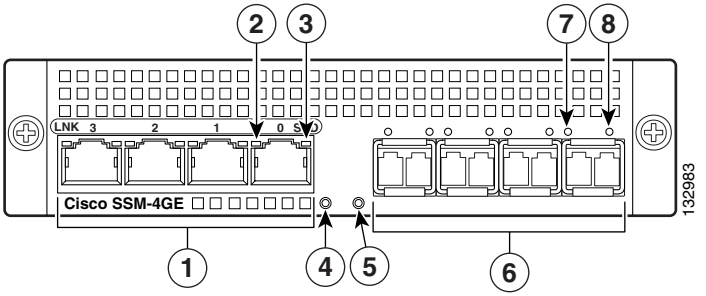
The 4GE Security Services Module (SSM) has eight Ethernet ports: four 10/100/1000 Mbps, copper, RJ-45 ports or four optional 1000 Mbps, Small Form-Factor Pluggable (SFP) fiber ports.

This section describes how to install and replace the Cisco 4GE SSM in the adaptive security appliance. This section includes the following topics:

4GE SSM Components

Figure 3-1 lists the Cisco 4GE SSM ports and LEDs.

Figure 3-1 Cisco 4GE SSM Ports and LEDs



1	RJ-45 ports	**5**	Status LED
2	RJ-45 Link LED	**6**	SFP ports
3	RJ-45 Speed LED	**7**	SFP Link LED
4	Power LED	**8**	SFP Speed LED

Note Figure 3-1 shows SFP modules installed in the port slots. You must order and install the SFP modules if you want to use this feature. For more information on SFP ports and modules, see the "Installing the SFP Modules" section on page 3-4.

Table 3-1 describes the Cisco 4GE SSM LEDs.

Table 3-1 Cisco 4GE SSM LEDs

	LED	Color	State	Description
2, 7	LINK	Green	Solid	There is an Ethernet link.
			Flashing	There is Ethernet activity.

Table 3-1 Cisco 4GE SSM LEDs (continued)

	LED	Color	State	Description
3, 8	SPEED	Off	10 MB	There is no network activity.
		Green	100 MB	There is network activity at 100 Mbps.
		Amber	1000 MB (GigE)	There is network activity at 1000 Mbps.
4	POWER	Green	On	The system has power.
5	STATUS	Green	Flashing	The system is booting.
		Green	Solid	The system booted correctly.
		Amber	Solid	The system diagnostics failed.

Installing the Cisco 4GE SSM

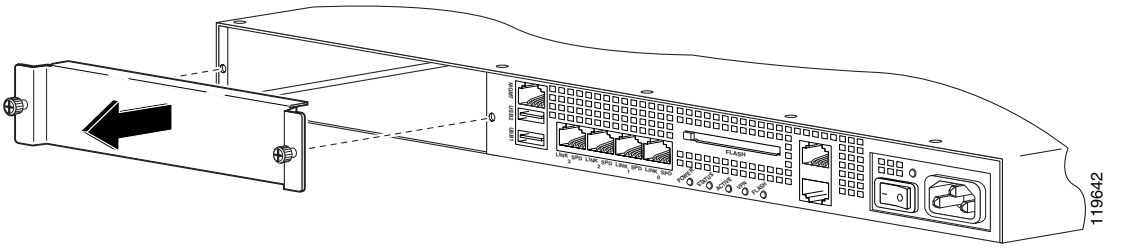
To install a new Cisco 4GE SSM for the first time, perform the following steps:

Step 1 Power off the adaptive security appliance.

Step 2 Locate the grounding strap from the accessory kit and fasten it to your wrist so that it contacts your bare skin. Attach the other end to the chassis.

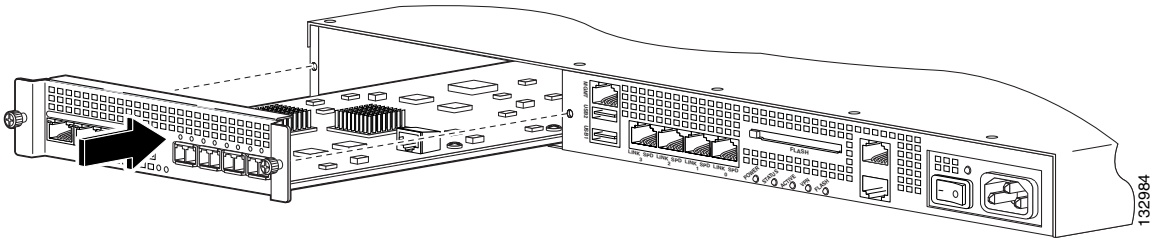
Step 3 Remove the two screws (as shown in Figure 3-2) at the left rear end of the chassis, and remove the slot cover.

Figure 3-2 Removing the Screws from the Slot Cover



Step 4 Insert the Cisco 4GE SSM through the slot opening as shown in Figure 3-3.

Figure 3-3 Inserting the Cisco 4GE SSM into the Slot



Step 5 Attach the screws to secure the Cisco 4GE SSM to the chassis.

Step 6 Power on the adaptive security appliance.

Step 7 Check the LEDs. If the Cisco 4GE SSM is installed properly the STATUS LED flashes during boot up and is solid when operational.

Step 8 Connect one end of the RJ-45 cable to the port and the other end of the cable to your network devices. For more information, see "Chapter 4, "Connecting Interface Cables."

Installing the SFP Modules

The SFP (Small Form-Factor Pluggable) is a hot-swappable input/output device that plugs into the SFP ports. The following SFP module types are supported:

- Long wavelength/long haul 1000BASE-LX/LH (GLC-LH-SM=)
- Short wavelength 1000BASE-SX (GLC-SX-MM=)

This section describes how to install and remove the SFP modules in the adaptive security appliance to provide optical Gigabit Ethernet connectivity. This section contains the following topics:

SFP Module

The adaptive security appliance uses a field-replaceable SFP module to establish Gigabit connections.

Note If you install an SFP module after the switch has powered on, you must reload the adaptive security appliance to enable the SFP module.

Table 3-2 lists the SFP modules that are supported by the adaptive security appliance.

Table 3-2 Supported SFP Modules

SFP Module	Type of Connection	Cisco Part Number
1000BASE-LX/LH	Fiber-optic	GLC-LH-SM=
1000BASE-SX	Fiber-optic	GLC-SX-MM=

The 1000BASE-LX/LH and 1000BASE-SX SFP modules are used to establish fiber-optic connections. Use fiber-optic cables with LC connectors to connect to an SFP module. The SFP modules support 850 to 1550 nm nominal wavelengths. The cables must not exceed the required cable length for reliable communications. Table 3-3 lists the cable length requirements.

Table 3-3 Cabling Requirements for Fiber-Optic SFP Modules

SFP Module	62.5/125 micron Multimode 850 nm Fiber	50/125 micron Multimode 850 nm Fiber	62.5/125 micron Multimode 1310 nm Fiber	50/125 micron Multimode 1310 nm Fiber	9/125 micron Single-mode 1310 nm Fiber
LX/LH	—	—	550 m at 500 Mhz-km	550 m at 400 Mhz-km	10 km
SX	275 m at 200 Mhz-km	550 m at 500 Mhz-km	—	—	—

Use only Cisco-certified SFP modules on the adaptive security appliance. Each SFP module has an internal serial EEPROM that is encoded with security information. This encoding provides a way for Cisco to identify and validate that the SFP module meets the requirements for the adaptive security appliance.

Note Only SFP modules certified by Cisco are supported on the adaptive security appliance.

Caution Protect your SFP modules by inserting clean dust plugs into the SFPs after the cables are extracted from them. Be sure to clean the optic surfaces of the fiber cables before you plug them back in the optical bores of another SFP module. Avoid getting dust and other contaminants into the optical bores of your SFP modules: The optics do not work correctly when obstructed with dust.

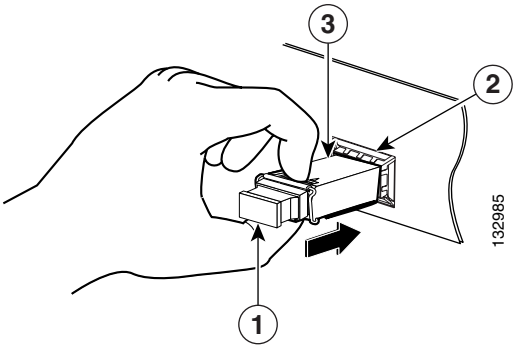
Warning **Because invisible laser radiation may be emitted from the aperture of the port when no cable is connected, avoid exposure to laser radiation and do not stare into open apertures.** Statement 70

Installing the SFP Module

To install the SFP module in the Cisco 4GE SSM, perform the following steps:

Step 1 Line up the SFP module with the port and slide the SFP module into the port slot until it locks into position as shown in Figure 3-4.

Figure 3-4 Installing an SFP Module



1	Optical port plug	**3**	SFP module
2	SFP port slot		

Caution Do not remove the optical port plugs from the SFP until you are ready to connect the cables.

Step 2 Remove the Optical port plug; then connect the network cable to the SFP module.

Connect the other end of the cable to your network. For more information on connecting the cables, see Chapter 4, "Connecting Interface Cables."

Caution The latching mechanism used on many SFPs locks them into place when cables are connected. Do not pull on the cabling in an attempt to remove the SFP.

Cisco AIP SSM and CSC SSM

The ASA 5500 series adaptive security appliance supports the AIP SSM (Advanced Inspection and Prevention Security Services Module) and the CSC SSM (Content Security Control Security Services Module), also referred to as the intelligent SSM.

The AIP SSM runs advanced IPS software that provides security inspection. There are two models of the AIP SSM: the AIP SSM 10 and the AIP SSM 20. Both types look identical, but the AIP SSM 20 has a faster processor and more memory than the AIP SSM 10. Only one module (the AIP SSM 10 or the AIP SSM 20) can populate the slot at a time.

Table 3-4 lists the memory specifications for the AIP SSM 10 and the AIP SSM 20.

Table 3-4 SSM Memory Specifications

SSM	CPU	DRAM
AIP SSM 10	2.0 GHz Celeron	1.0 GB
AIP SSM 20	2.4 GHz Pentium 4	2.0 GB

For more information on the AIP SSM, see the "Managing the AIP SSM" section in the *Cisco Security Appliance Command Line Configuration Guide.*

The CSC SSM runs Content Security and Control software. The CSC SSM provides protection against viruses, spyware, spam, and other unwanted traffic. For more information on the CSC SSM, see the "Managing the CSC SSM" section in the *Cisco Security Appliance Command Line Configuration Guide.*

This section describes how to install and replace the SSM in the adaptive security appliance. Figure 3-5 lists the SSM LEDs.

Figure 3-5 SSM LEDs

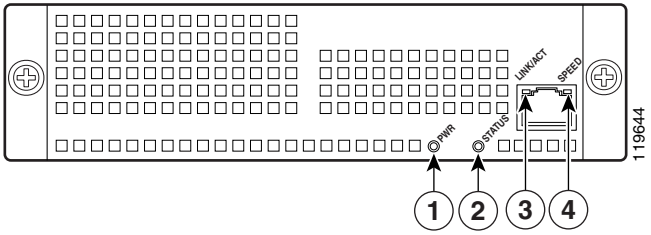


Table 3-5 describes the SSM LEDs.

Table 3-5 SSM LEDs

	LED	Color	State	Description
1	PWR	Green	On	The system has power.
2	STATUS	Green	Flashing	The system is booting.
			Solid	The system has passed power-up diagnostics.
3	LINK/ACT	Green	Solid	There is an Ethernet link.
			Flashing	There is Ethernet activity.
4	SPEED	Green	100 MB	There is network activity.
		Amber	1000 MB (GigE)	There is network activity.

Installing an SSM

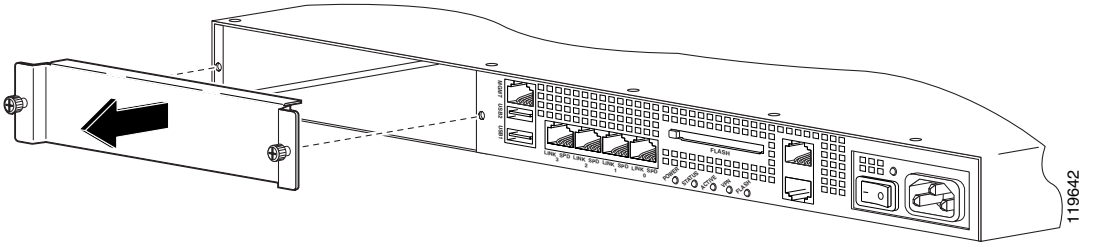
To install a new SSM, perform the following steps:

Step 1 Power off the adaptive security appliance.

Step 2 Locate the grounding strap from the accessory kit and fasten it to your wrist so that it contacts your bare skin. Attach the other end to the chassis.

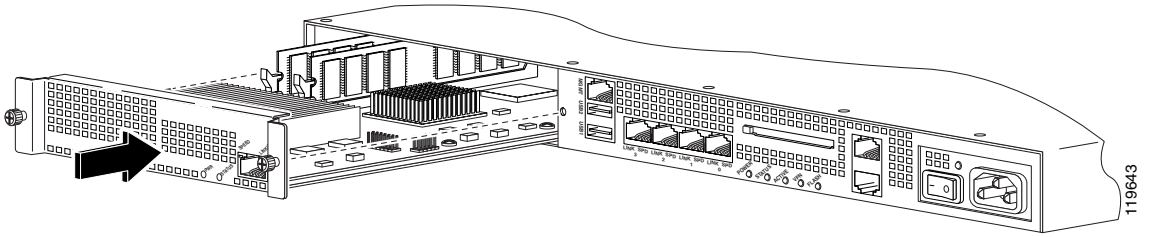
Step 3 Remove the two screws (as shown in Figure 3-6) at the left rear end of the chassis, and remove the slot cover.

Figure 3-6 Removing the Screws from the Slot Cover



Step 4 Insert the SSM into the slot opening as shown in Figure 3-7.

Figure 3-7 Inserting the SSM into the Slot



Step 5 Attach the screws to secure the SSM to the chassis.

Step 6 Power on the adaptive security appliance. Check the LEDs. If the SSM is installed properly the POWER LED is solid green and the STATUS LED flashes green.

Step 7 Connect one end of the RJ-45 cable to the port and the other end of the cable to your network devices.

What to Do Next

Continue with Chapter 4, "Connecting Interface Cables."

Connecting Interface Cables

This chapter describes how to connect the cables to the Console, Auxiliary, Management, Cisco 4GE SSM, and SSM ports. In this document, SSM refers to an intelligent SSM, the AIP SSM, or the CSC SSM.

This chapter includes the following sections:

Note The 4GE SSM, AIP SSM, and CSC SSM are optional security services modules. Skip these steps if your adaptive security appliance does not include these modules.

Warning **Only trained and qualified personnel should install, replace, or service this equipment.** Statement 49

Caution Read the safety warnings in the *Regulatory Compliance and Safety Information for the Cisco ASA 5500 Series* and follow proper safety procedures when performing these steps.

Connecting Cables to Interfaces

To connect cables to the interfaces, perform the following steps:

Step 1 Place the chassis on a flat, stable surface, or in a rack (if you are rack-mounting it).

Step 2 Before connecting a computer or terminal to the ports, check to determine the baud rate of the serial port. The baud rate must match the default baud rate (9600 baud) of the Console port of the adaptive security appliance. Set up the terminal as follows: 9600 baud (default), 8 data bits, no parity, 1 stop bits, and Flow Control (FC) = Hardware.

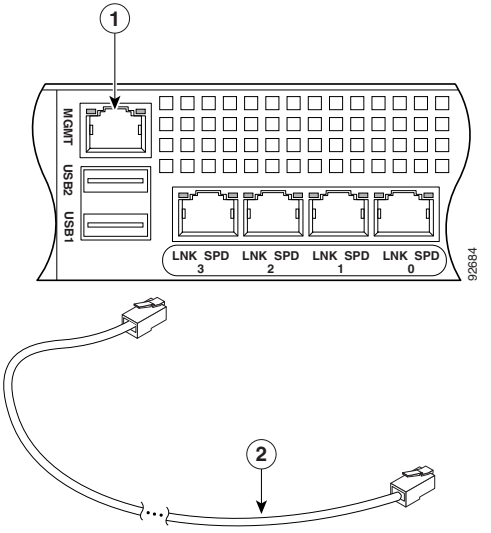
Step 3 Connect the cables to the ports.

a. Management port–The adaptive security appliance has a dedicated management interface referred to as the Management0/0 port. The Management0/0 port is a Fast Ethernet interface with a dedicated port used only for traffic management. Similar to the Console port, but the Management port accepts only incoming traffic to the adaptive security appliance.

Note You can configure any interface to be a management-only interface using the **management-only** command. You can also disable management-only mode on the management interface. For more information about this command, see the **management-only** command in the *Cisco Security Appliance Command Reference*.

- Connect one RJ-45 connector to the Management0/0 port, as shown in Figure 4-1.
- Connect the other end of the Ethernet cable to the Ethernet port on your computer.

Figure 4-1 Connecting to the Management Port

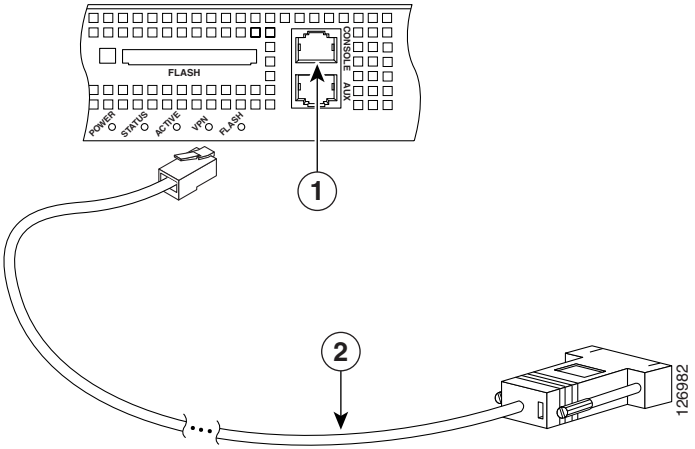


1	Management port	**2**	RJ-45 to RJ-45 Ethernet cable

b. Console port

- Connect the serial console cable as shown in Figure 4-2. The console cable has a DB-9 connector on one end for the serial port on your computer, and the other end is an RJ-45 connector.
- Connect the RJ-45 connector to the Console port on the adaptive security appliance.
- Connect the other end of the cable, the DB-9 connector, to the console port on your computer.

Figure 4-2 Connecting the Console Cable

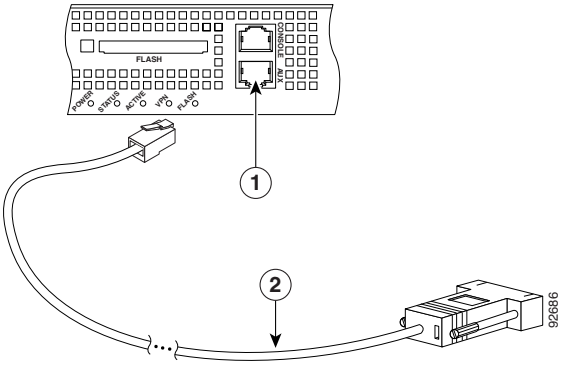


1	RJ-45 Console port	**2**	RJ-45 to DB-9 console cable

c. Auxiliary port

- Connect the serial console cable as shown in Figure 4-2. The console cable has a DB-9 connector on one end for the serial port on your computer, and the other end is an RJ-45 connector.
- Connect the RJ-45 connector to the Auxiliary port (labeled AUX) on the adaptive security appliance, as shown in Figure 4-3.
- Connect the other end of the cable, the DB-9 connector, to the serial port on your computer.

Figure 4-3 Connecting to the AUX Port



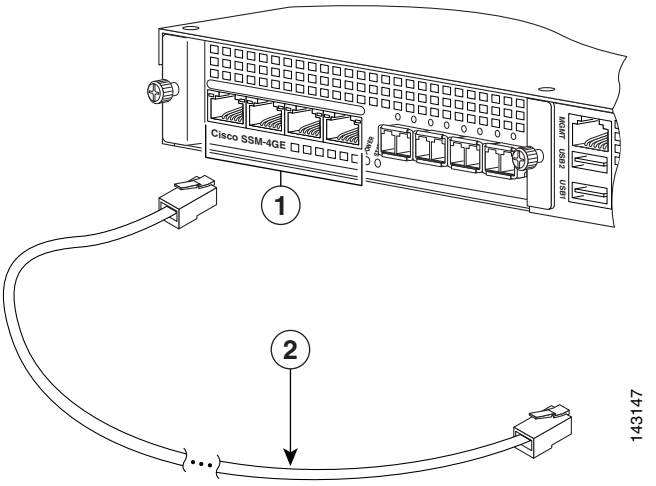
1	RJ-45 AUX port	**2**	RJ-45 to DB-9 console cable

d. Cisco 4GE SSM

- Ethernet port
  - Connect one RJ-45 connector to the Ethernet port of the Cisco 4GE SSM as shown in Figure 4-4.
  - Connect the other end of the Ethernet cable to your network device, such as a router, switch or hub.

Note The Cisco 4GE SSM is optional; this connection is necessary only if you have installed the Cisco 4GE SSM on the adaptive security appliance.

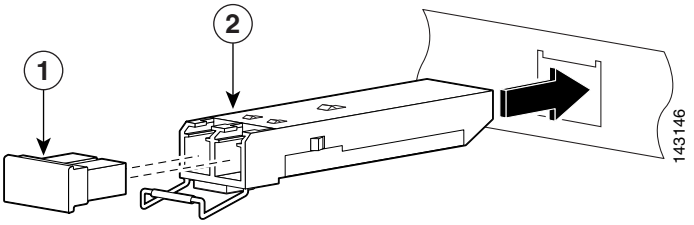
Figure 4-4 Connecting to the RJ-45 port



1	Ethernet ports	**2**	RJ-45 connector

- SFP modules
  - Insert and slide the SFP module into the SFP port until you hear a click. The click indicates that the SFP module is locked into the port.
  - Remove the optical port plugs from the installed SFP as shown in Figure 4-5.

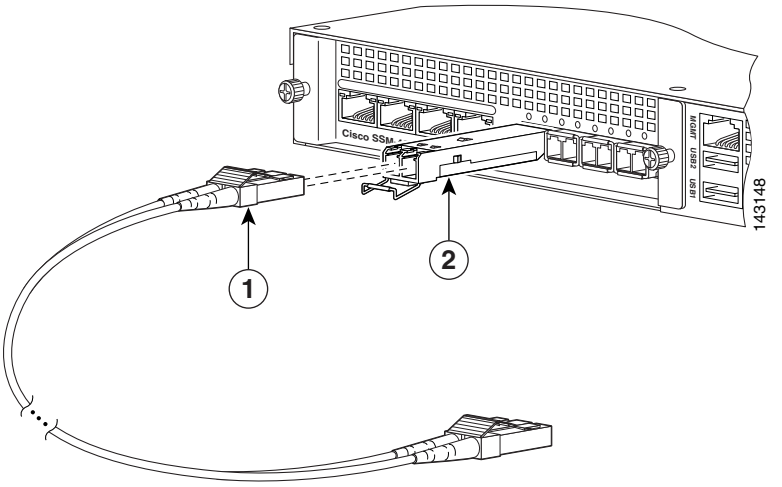
Figure 4-5 Removing the Optical Port Plug



1	Optical port plug	**2**	SFP module

  - Connect the LC connector to the SFP module as shown in Figure 4-6.

Figure 4-6 Connecting the LC Connector



1	LC connector	**2**	SFP module

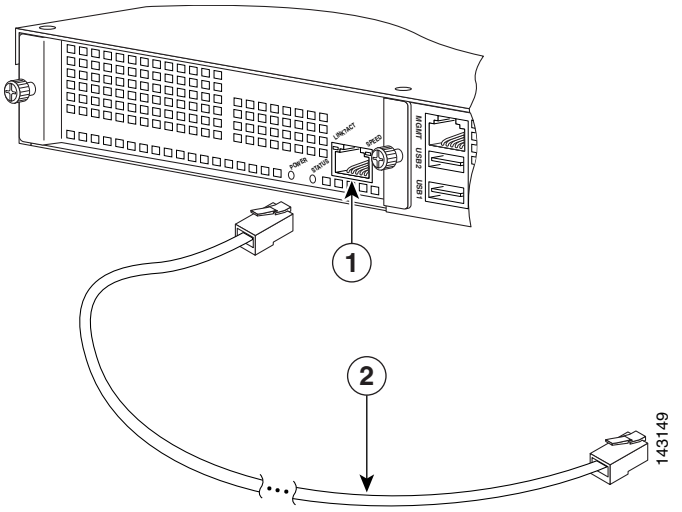
- Connect the other end to your network devices, such as routers, switches, or hubs.

e. SSM

- Connect one RJ-45 connector to the management port on the SSM, as shown in Figure 4-7.
- Connect the other end of the RJ-45 cable to your network devices.

Note SSMs are optional; this connection is necessary only if you have installed an SSM on the adaptive security appliance.

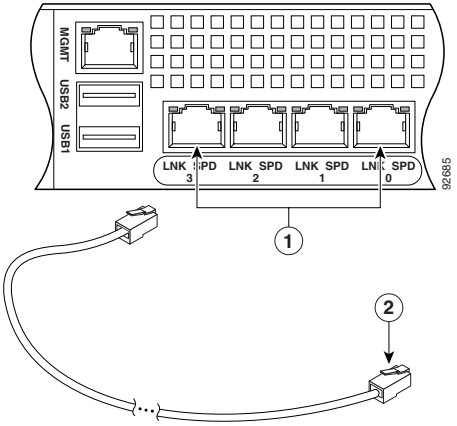
Figure 4-7 Connecting to the Management Port



1	SSM management port	**2**	RJ-45 to RJ-45 cable

f. Ethernet ports
   - Connect the RJ-45 connector to the Ethernet port as shown in Figure 4-8.
   - Connect the other end of the Ethernet cable to your network device, such as a router, switch or hub.

Figure 4-8 Connecting Cables to Network Interfaces



1	RJ-45 Ethernet ports	**2**	RJ-45 connector

Step 4 Connect the power cord to the adaptive security appliance and plug the other end to the power source.

Step 5 Power on the chassis.

What to Do Next

Continue with Chapter 5, "Configuring the Adaptive Security Appliance."

Configuring the Adaptive Security Appliance

This chapter describes the initial configuration of the adaptive security appliance. You can perform the configuration steps using either the browser-based Cisco Adaptive Security Device Manager (ASDM) or the command-line interface (CLI). However, the procedures in this chapter refer to the method using ASDM.

Note To use ASDM, you must have a DES license or a 3DES-AES license. For more information, see Appendix A, "Obtaining a DES License or a 3DES-AES License."

This chapter includes the following sections:

About the Factory-Default Configuration

Cisco adaptive security appliances are shipped with a factory-default configuration that enables quick startup. This configuration meets the needs of most small and medium business networking environments.

By default, the adaptive security appliance Management interface is configured with a default DHCP address pool. This configuration enables a client on the inside network to obtain a DHCP address from the adaptive security appliance to connect to the appliance. Administrators can then configure and manage the adaptive security appliance using ASDM. Based on your network security policy, you should also consider configuring the adaptive security appliance to deny all ICMP traffic through the outside interface or any other interface that is necessary.

About the Adaptive Security Device Manager

The Adaptive Security Device Manager (ASDM) is a feature-rich graphical interface that enables you to manage and monitor the adaptive security appliance. Its web-based design provides secure access so that you can connect to and manage the adaptive security appliance from any location by using a web browser.

In addition to its complete configuration and management capability, ASDM features intelligent wizards to simplify and accelerate the deployment of the adaptive security appliance.

To use ASDM, you must have a DES license or a 3DES-AES license. In addition, Java and JavaScript must be enabled in your web browser.

In addition to the ASDM web configuration tool, you can configure the adaptive security appliance by using the command-line interface. For more information, see the *Cisco Security Appliance Command Line Configuration Guide* and the *Cisco Security Appliance Command Reference*.

Before Launching the Startup Wizard

Before you launch the Startup Wizard, perform the following steps:

Step 1 Obtain a DES license or a 3DES-AES license.

To run ASDM, you must have a DES license or a 3DES-AES license. If you did not purchase one of these licenses with the adaptive security appliance, see Appendix A, "Obtaining a DES License or a 3DES-AES License" for information about how to obtain and activate one.

Step 2 Enable Java and Javascript in your Web browser.

Step 3 Gather the following information:

- A unique hostname to identify the adaptive security appliance on your network.
- The IP addresses of your outside interface, inside interface, and any other interfaces.
- The IP addresses to use for NAT or PAT configuration.
- The IP address range for the DHCP server.

Using the Startup Wizard

ASDM includes a Startup Wizard to simplify the initial configuration of your adaptive security appliance. With a few steps, the Startup Wizard enables you to configure the adaptive security appliance so that it allows packets to flow securely between the inside network (GigabitEthernet0/1) and the outside network (GigabitEthernet0/0).

To use the Startup Wizard to set up a basic configuration for the adaptive security appliance, perform the following steps:

Step 1 If you have not already done so, perform one of the following steps:

- If you have an ASA 5520 or 5540, connect the inside GigabitEthernet0/1 interface to a switch or hub by using the Ethernet cable. To this same switch, connect a PC for configuring the adaptive security appliance.
- If you have an ASA 5510, connect the inside Ethernet 1 interface to a switch or hub by using the Ethernet cable. To this same switch, connect a PC for configuring the adaptive security appliance.

Step 2 Configure your PC to use DHCP (to receive an IP address automatically from the adaptive security appliance), or assign a static IP address to your PC by selecting an address out of the 192.168.1.0 network. (Valid addresses are 192.168.1.2 through 192.168.1.254, with a mask of 255.255.255.0 and default route of 192.168.1.1.)

Note The inside interface of the adaptive security appliance is assigned 192.168.1.1 by default, so this address is unavailable.

Step 3 Perform one of the following steps:

- If you have an ASA 5520 or 5540, check the LINK LED on the GigabitEthernet0/1 interface.
- If you have an ASA 5510, check the LINK LED on the Ethernet 1 interface.

When a connection is established, the LINK LED interface on the adaptive security appliance and the corresponding LINK LED on the switch or hub becomes solid green.

Step 4 Launch the Startup Wizard.

a. On the PC connected to the switch or hub, launch an Internet browser.

b. In the address field of the browser, enter this URL: **https://192.168.1.1/**.

Note The adaptive security appliance ships with a default IP address of 192.168.1.1. Remember to add the "**s**" in "**https**" or the connection fails. HTTPS (HTTP over SSL) provides a secure connection between your browser and the adaptive security appliance.

Step 5 In the dialog box that requires a username and password, leave both fields empty. Press **Enter**.

Step 6 Click **Yes** to accept the certificates. Click **Yes** for all subsequent authentication and certificate dialog boxes.

ASDM starts.

Step 7 From the Wizards menu at the top of the ASDM window, choose Startup Wizard.

Step 8 Follow the instructions in the Startup Wizard to set up your adaptive security appliance.

For information about any field in the Startup Wizard, click **Help** at the bottom of the window.

What to Do Next

Next, configure the adaptive security appliance for your deployment using one or more of the following chapters:

To Do This ...	See ...
Configure the adaptive security appliance to protect a DMZ web server	Chapter 6, "Scenario: DMZ Configuration"
Configure the adaptive security appliance for remote-access VPN	Chapter 7, "Scenario: Remote-Access VPN Configuration"
Configure the adaptive security appliance for Site-to-Site VPN	Chapter 8, "Scenario: Site-to-Site VPN Configuration"

To Do This ...	See ...
Configure the AIP SSM for intrusion prevention	Chapter 9, "Configuring the AIP SSM"
Configure the CSC SSM for content security	Chapter 10, "Configuring the CSC SSM"

Scenario: DMZ Configuration

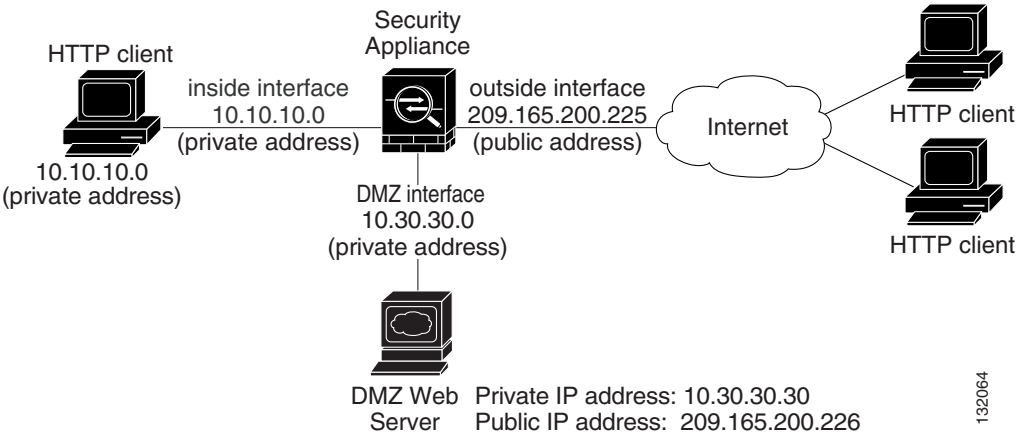
This chapter describes a configuration scenario in which the adaptive security appliance is used to protect network resources located in a demilitarized zone (DMZ). A DMZ is a separate network located in the neutral zone between a private (inside) network and a public (outside) network.

This chapter includes the following sections:

Example DMZ Network Topology

The example network topology shown in Figure 6-1 is typical of most DMZ implementations of the adaptive security appliance.

Figure 6-1 Network Layout for DMZ Configuration Scenario

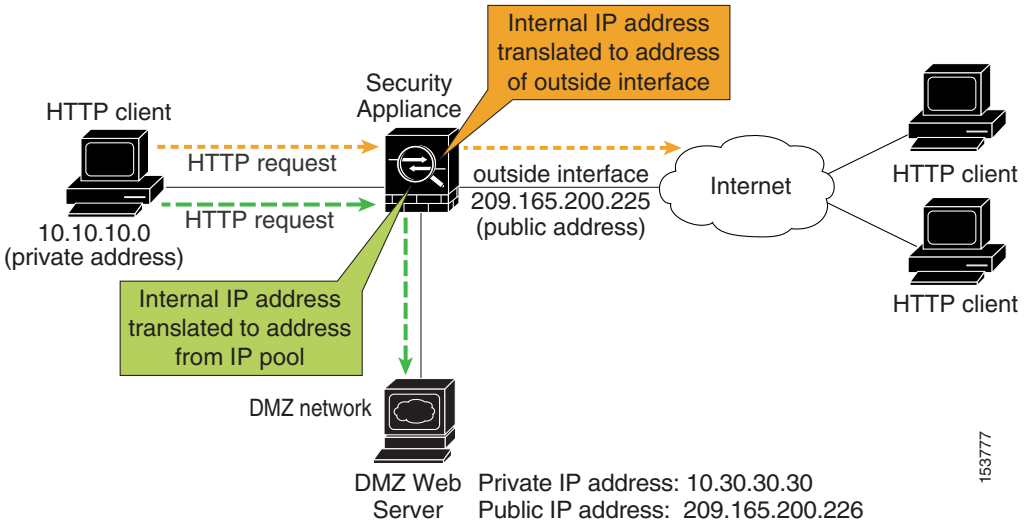


This example scenario has the following characteristics:

- The web server is on the DMZ interface of the adaptive security appliance.
- HTTP clients on the private network can access the web server in the DMZ and can also communicate with devices on the Internet.
- Clients on the Internet are permitted HTTP access to the DMZ web server; all other traffic is denied.
- The network has two routable IP addresses that are publicly available: one for the outside interface of the adaptive security appliance (209.165.200.225), and one for the public IP address of the DMZ web server (209.165.200.226).

Figure 6-2 shows the outgoing traffic flow of HTTP requests from the private network to both the DMZ web server and to the Internet.

Figure 6-2 Outgoing HTTP Traffic Flow from the Private Network



In Figure 6-2, the adaptive security appliance permits HTTP traffic originating from inside clients and destined for both the DMZ web server and devices on the Internet. To permit the traffic through, the adaptive security appliance configuration includes the following:

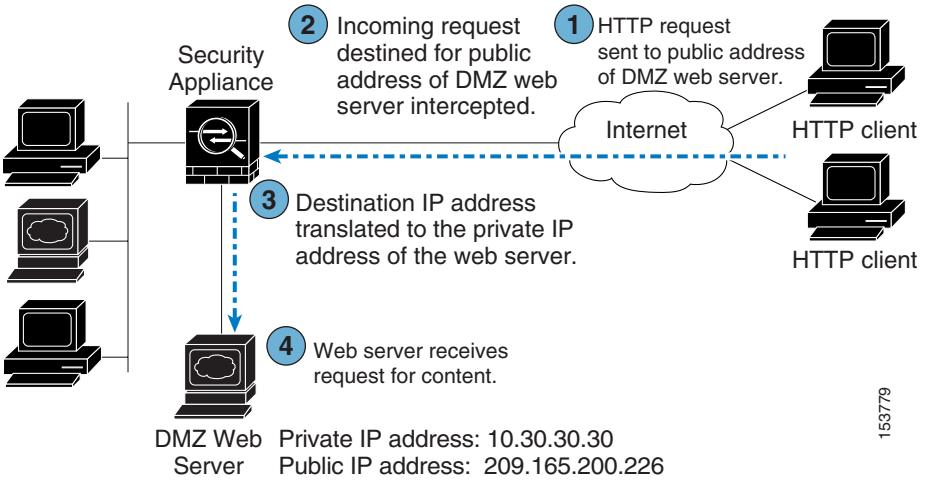
- Access control rules permitting traffic destined for the DMZ web server and for devices on the Internet.
- Address translation rules translating private IP addresses so that the private addresses are not visible to the Internet.

  For traffic destined for the DMZ web server, private IP addresses are translated to an address from an IP pool.

  For traffic destined for the Internet, private IP addresses are translated to the public IP address of the adaptive security appliance. Outgoing traffic appears to come from this address.

Figure 6-3 shows HTTP requests originating from the Internet and destined for the public IP address of the DMZ web server.

Figure 6-3 Incoming HTTP Traffic Flow From the Internet



To permit incoming traffic to access the DMZ web server, the adaptive security appliance configuration includes the following:

- An address translation rule translating the public IP address of the DMZ web server to the private IP address of the DMZ web server.
- An access control rule permitting incoming HTTP traffic that is destined for the DMZ web server.

The procedures for creating this configuration are detailed in the remainder of this chapter.

Configuring the Security Appliance for a DMZ Deployment

This section describes how to use ASDM to configure the adaptive security appliance for the configuration scenario shown in Figure 6-1. The procedure uses sample parameters based on the scenario.

This configuration procedure assumes that the adaptive security appliance already has interfaces configured for the inside interface, the DMZ interface, and the outside interface. Set up interfaces of the adaptive security appliance by using the Startup Wizard in ASDM. Be sure that the DMZ interface security level is set between 0 and 100. (A common choice is 50.)

For more information about using the Startup Wizard, see Chapter 5, "Configuring the Adaptive Security Appliance."

The section includes the following topics:

The following sections provide detailed instructions for how to perform each step.

Configuration Requirements

Configuring the adaptive security appliance for this DMZ deployment requires the following configuration tasks:

- For the internal clients to have HTTP access to the DMZ web server, you must create a pool of IP addresses for address translation and identify which clients should use addresses from the pool. To accomplish this task, you should configure the following:
  - A pool of IP addresses for the DMZ interface. In this scenario, the IP pool is 10.30.30.50–10.30.30.60.
  - A dynamic NAT translation rule for the inside interface that specifies which client IP addresses can be assigned an address from the IP pool.

- For the internal clients to have access to HTTP and HTTPS resources on the Internet, you must create a rule that translates the real IP addresses of internal clients to an external address that can be used as the source address.

  To accomplish this task, you should configure a PAT translation rule (port address translation rule, sometimes called an interface NAT) for the internal interface that translates internal IP addresses to the external IP address of the adaptive security appliance.

  In this scenario, the internal address to be translated is that of a subnet of the private network (10.10.10.0). Addresses from this subnet are translated to the public address of the adaptive security appliance (209.165.200.225).

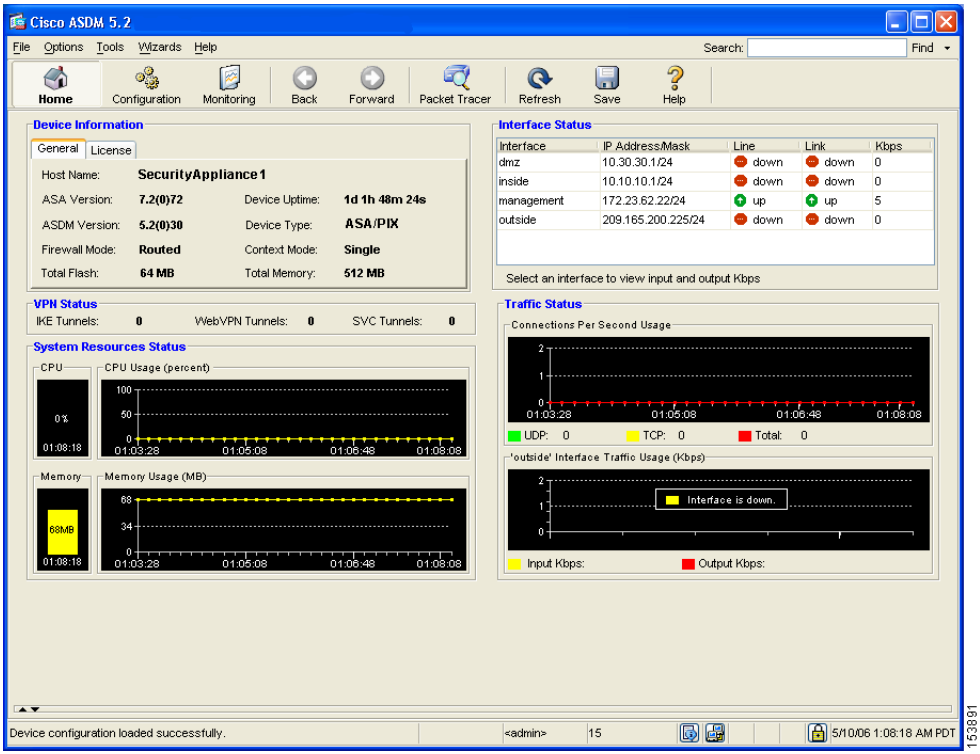
- For external clients to have HTTP access to the DMZ web server, you must configure an external identity for the DMZ web server and an access rule that permits HTTP requests coming from clients on the Internet. To accomplish this task, you should configure the following:
  - Create a static NAT rule. This rule translates the real IP address of the DMZ web server to a single public IP address. In this scenario, the public address of the web server is 209.165.200.226.
  - Create a security access rule permitting traffic from the Internet if the traffic is an HTTP request destined for the public IP address of the DMZ web server.

Starting ASDM

To run ASDM in a web browser, enter the factory-default IP address in the address field: **https://192.168.1.1/admin/**.

Note Remember to add the "**s**" in "**https**" or the connection fails. HTTPS (HTTP over SSL) provides a secure connection between your browser and the adaptive security appliance.

The Main ASDM window appears.



Creating IP Pools for Network Address Translation

The adaptive security appliance uses Network Address Translation (NAT) and Port Address Translation (PAT) to prevent internal IP addresses from being exposed externally. This procedure describes how to create a pool of IP addresses that the DMZ interface and outside interface can use for address translation.

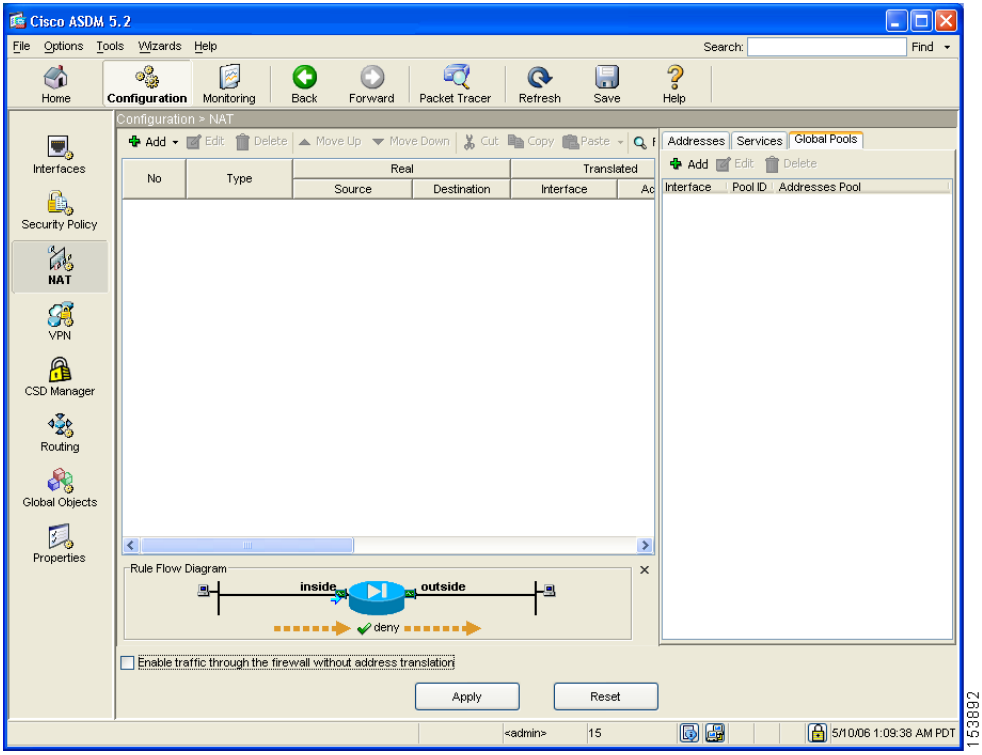
A single IP pool can contain both NAT and PAT entries, and it can contain entries for more than one interface.

To configure a pool of IP addresses that can be used for network address translation, perform the following steps:

Step 1 In the ASDM window, click the **Configuration** tool.

a. In the Features pane, click **NAT**.

The NAT Configuration screen appears.

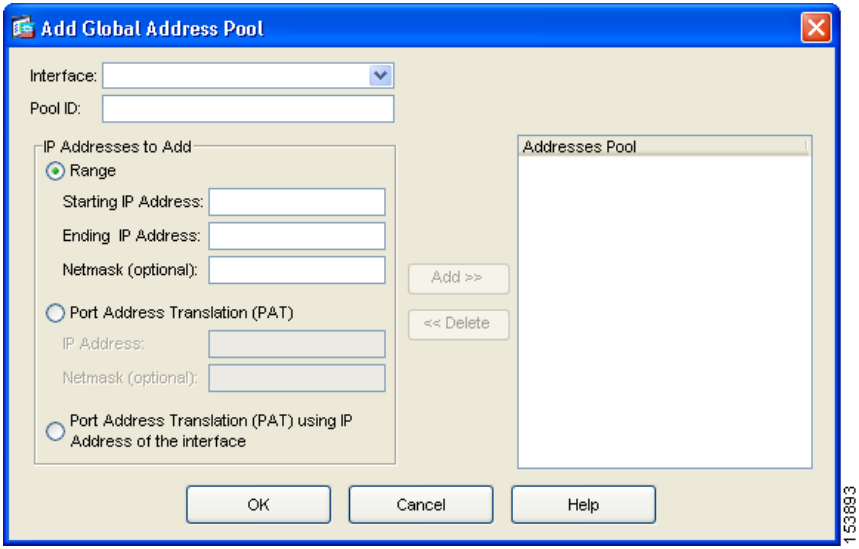


b. In the right pane, click the **Global Pools** tab.

c. Click **Add** to create a new global pool for the DMZ interface.

The Add Global Address Pool dialog box appears.

Note For most configurations, IP pools are added to the less secure, or public, interfaces.



d. From the Interfaces drop-down list, choose DMZ.

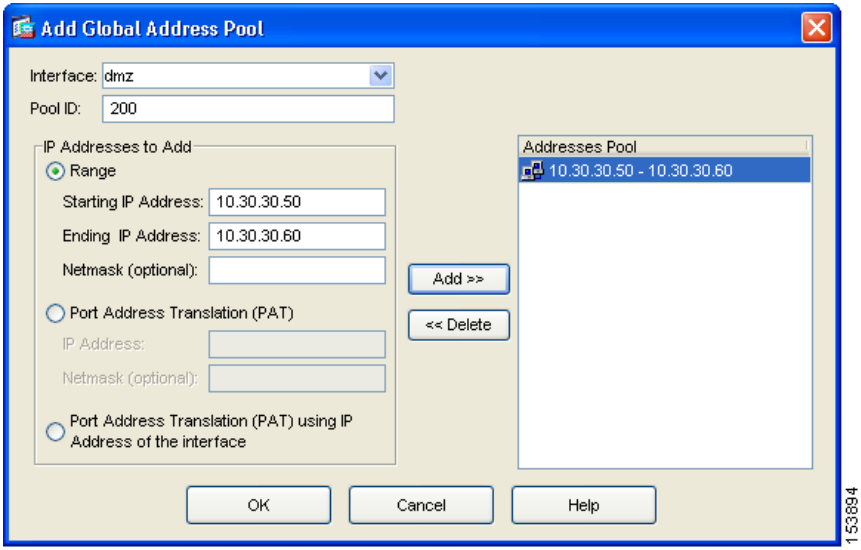
e. To create a new IP pool, enter a unique Pool ID. In this scenario, the Pool ID is 200.

f. In the IP Addresses to Add area, specify the range of IP addresses to be used by the DMZ interface:

- Click the **Range** radio button.
- Enter the Starting IP address and Ending IP address of the range. In this scenario, the range of IP addresses is 10.30.30.50–10.30.30.60.
- (Optional) Enter the Netmask for the range of IP addresses.

g. Click **Add** to add this range of IP addresses to the Address Pool.

The Add Global Pool dialog box configuration should be similar to the following:



h. Click **OK** to return to the Configuration > NAT window.

Step 2 Add addresses to the IP pool to be used by the outside interface. These addresses are used to translate private IP addresses so that inside clients can communicate securely with clients on the Internet.

In this scenario, there are limited public IP addresses available. Use Port Address Translation (PAT) so that many internal IP addresses can map to the same public IP address, as follows:

a. In the right pane of the NAT Configuration screen, click the **Global Pools** tab.

b. Under the Global Pools tab, click **Add**.

The Add Global Pool Item dialog box appears.

c. From the Interface drop-down list, choose Outside.

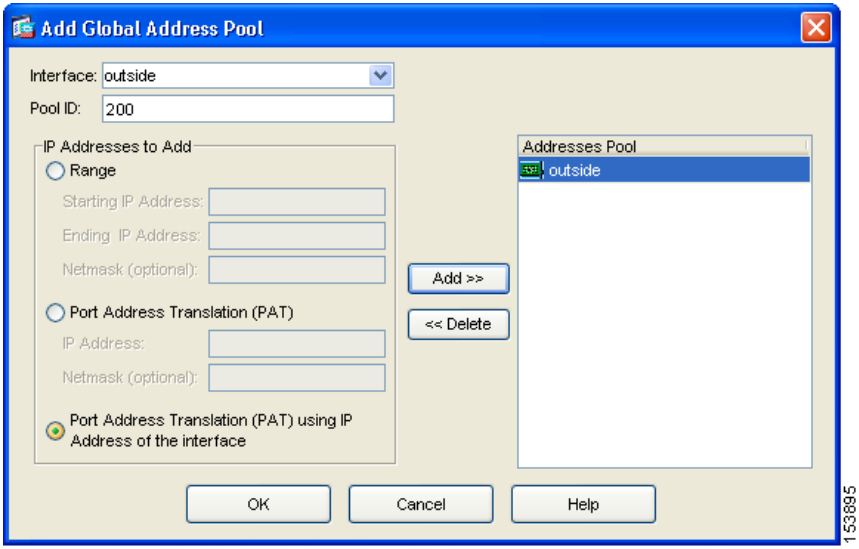
d. Specify a Pool ID for the Outside interface.

You can add these addresses to the same IP pool that contains the address pool used by the DMZ interface (in this scenario, the Pool ID is 200).

e. Click the **Port Address Translation (PAT) using the IP address of the interface** radio button.

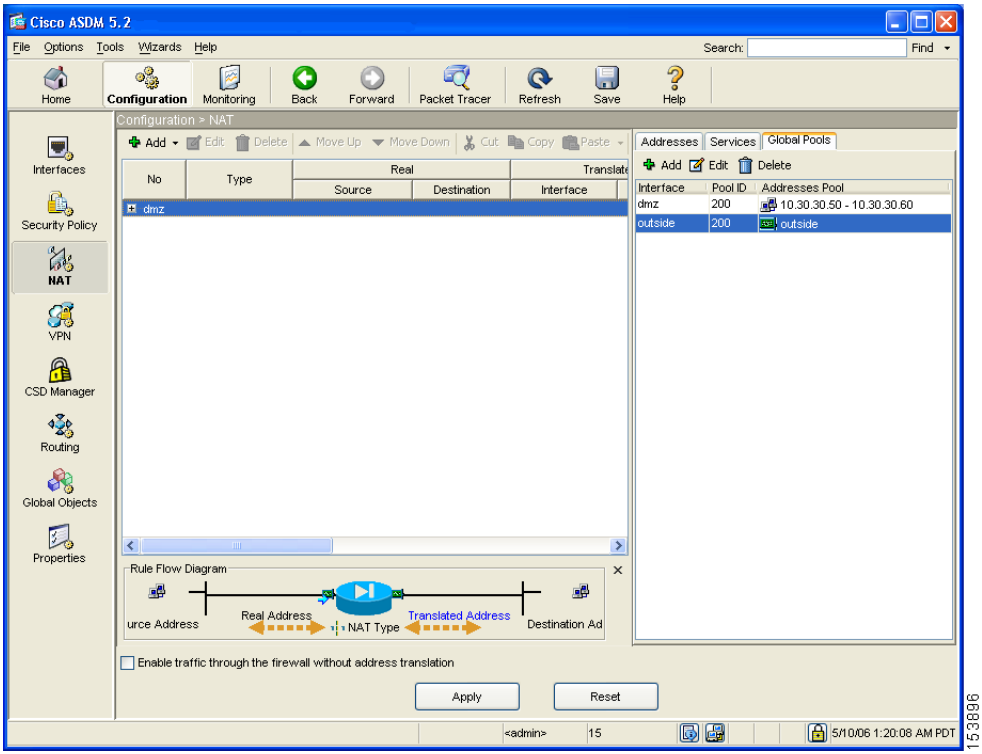
If you select the option Port Address Translation using the IP address of the interface, all traffic initiated from the inside network exits the adaptive security appliance using the IP address of the outside interface. To the devices on the Internet, it appears that all traffic is coming from this one IP address.

f. Click the **Add** button to add this new address to the IP pool.



g. Click **OK**.

The displayed configuration should be similar to the following:



Step 3 Confirm that the configuration values are correct.

Step 4 Click **Apply** in the main ASDM window.

Configuring NAT for Inside Clients to Communicate with the DMZ Web Server

In the previous procedure, you created a pool of IP addresses that could be used by the adaptive security appliance to mask the private IP addresses of inside clients.

In this procedure, you configure a Network Address Translation (NAT) rule that associates IP addresses from this pool with the inside clients so they can communicate securely with the DMZ web server.

To configure NAT between the inside interface and the DMZ interface, perform the following steps starting from the main ASDM window:

Step 1 In the main ASDM window, click the **Configuration** tool.

Step 2 In the Features pane, click **NAT**.

Step 3 From the Add drop-down list, choose Add Dynamic NAT Rule.

The Add Dynamic NAT Rule dialog box appears.

Step 4 In the Real Address area, specify the IP address to be translated. For this scenario, address translation for inside clients is done according to the IP address of the subnet.

a. From the Interface drop-down list, choose the Inside interface.

b. Enter the IP address of the client or network. In this scenario, the IP address of the network is 10.10.10.0.

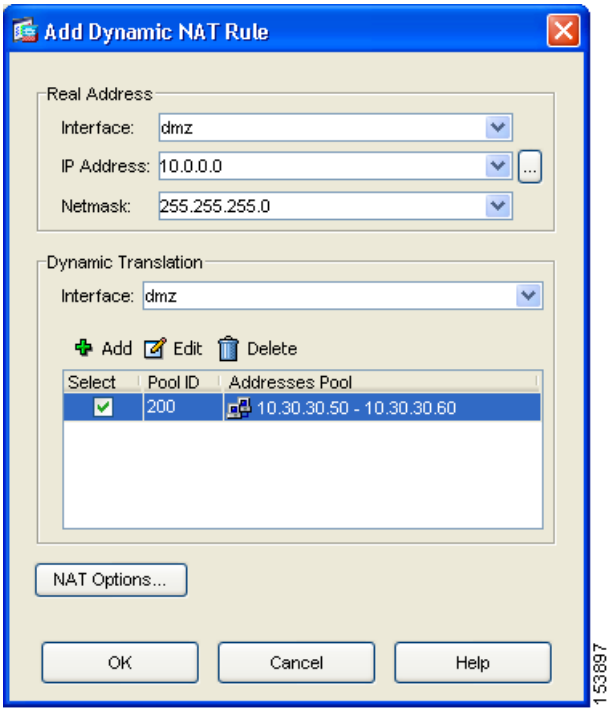
c. From the Netmask drop-down list, choose the Netmask. In this scenario, the netmask is 255.255.255.0.

Step 5 In the Dynamic Translation area:

a. From the Interface drop-down list, choose the DMZ interface.

b. To specify the address pool to be used for this Dynamic NAT rule, check the **Select** check box next to Global Pool ID. In this scenario, the IP pool ID is 200.

In this scenario, the IP pool that we want to use is already created. If it was not already created, you would click **Add** to create a new IP pool.



c. Click **OK** to add the Dynamic NAT Rule and return to the Configuration > NAT window.

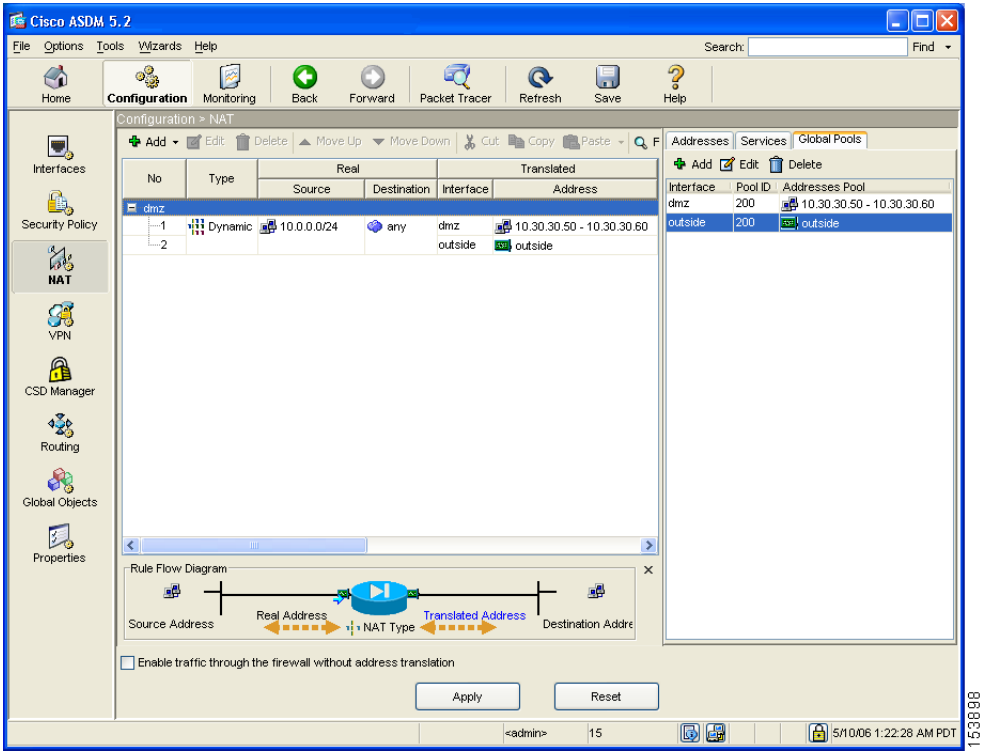
Review the configuration screen to verify that the translation rule appears as you expected.

Note When you click OK to create this rule, notice that there are actually two translation rules created:

- A translation rule between the inside and DMZ interfaces to be used when inside clients communicate with the DMZ web server.
- A translation rule between the inside and outside interfaces to be used when inside clients communicate with the Internet.

ASDM is able to create both rules because the addresses to be used for translation are both in the same IP pool.

The displayed configuration should be similar to the following:



Step 6 Click **Apply** to complete the adaptive security appliance configuration changes.

Configuring NAT for Inside Clients to Communicate with Devices on the Internet

In the previous procedure, you configured a Network Address Translation (NAT) rule that associates IP addresses from the IP pool with the inside clients so they can communicate securely with the DMZ web server.

For many configurations, you would also need to create a NAT rule between the inside interface and the outside interface to enable inside clients to communicate with the Internet.

However, in this scenario you do not need to create this rule explicitly. The reason is that the IP pool (pool ID 200) contains both types of addresses needed for address translation: the range of IP addresses to be used by the DMZ interface, and the IP address to be used for the outside interface. This enables ASDM to create the second translation rule for you.

Configuring an External Identity for the DMZ Web Server

The DMZ web server needs to be accessible by all hosts on the Internet. This configuration requires translating the private IP address of the DMZ web server to a public IP address, enabling access to outside HTTP clients that are unaware of the adaptive security appliance. To map the real web server IP address (10.30.30.30) statically to a public IP address (209.165.200.226), perform the following steps:

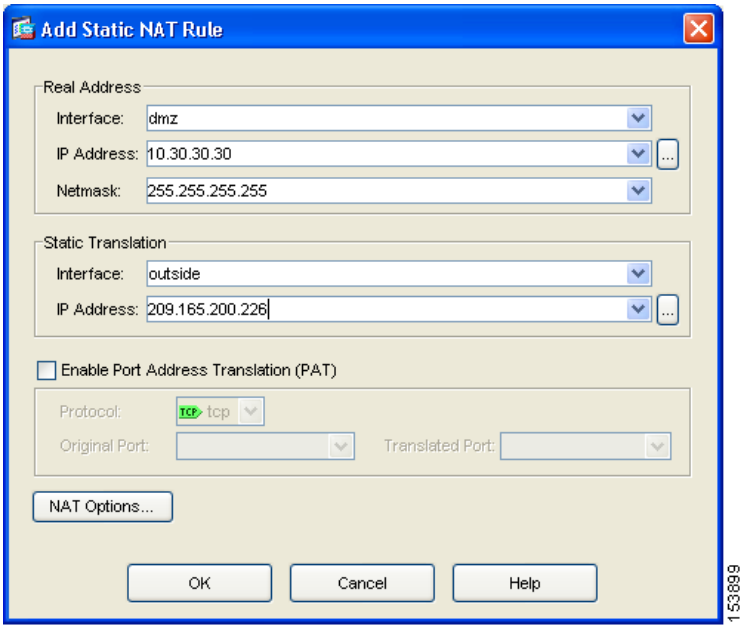
Step 1 In the ASDM window, click the **Configuration** tool.

Step 2 In the Features pane, click **NAT**.

Step 3 From the Add drop-down list, choose Add Static NAT Rule. The Add Static NAT Rule dialog box appears.

Step 4 In the Real Address area, specify the real IP address of the web server:

- **a.** From the Interface drop-down list, choose the DMZ interface.
- **b.** Enter the real IP address of the DMZ web server. In this scenario, the IP address is 10.30.30.30.
- **c.** From the Netmask drop-down list, choose the Netmask 255.255.255.255.



Step 5 In the Static Translation area, specify the public IP address to be used for the web server:

a. From the Interface drop-down list, choose Outside.

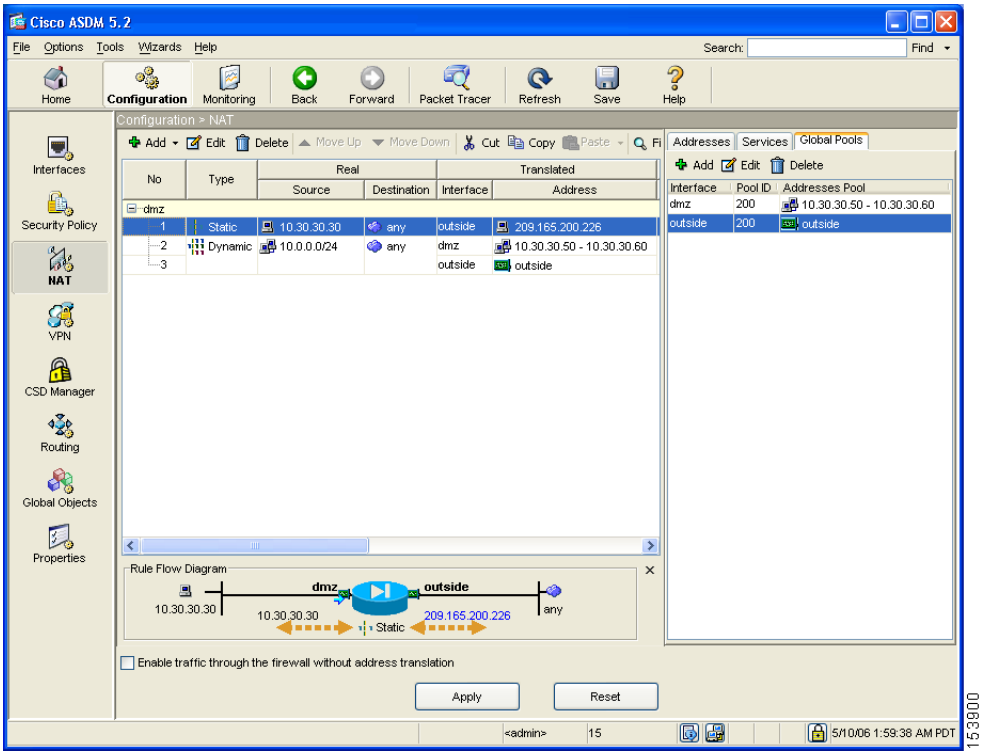
b. From the IP Address drop-down list, choose the public IP address of the DMZ web server.

In this scenario, the public IP address of the DMZ web server is 209.165.200.226.

Step 6 Click **OK** to add the rule and return to the list of Address Translation Rules.

This rule maps the real web server IP address (10.30.30.30) statically to the public IP address of the web server (209.165.200.226).

The displayed configuration should be similar to the following:



Step 7 Click **Apply** to complete the adaptive security appliance configuration changes.

Providing Public HTTP Access to the DMZ Web Server

By default, the adaptive security appliance denies all traffic coming in from the public network. You must create an access control rule on the adaptive security appliance to permit specific traffic types from the public network to resources in the DMZ. This access control rule specifies the interface of the adaptive security

appliance that processes the traffic, whether the traffic is incoming or outgoing, the origin and destination of the traffic, and the type of traffic protocol and service to be permitted.

In this section, you create an access rule that permits incoming HTTP traffic originating from any host or network on the Internet, if the destination of the traffic is the web server on the DMZ network. All other traffic coming in from the public network is denied.

To configure the access control rule, perform the following steps:

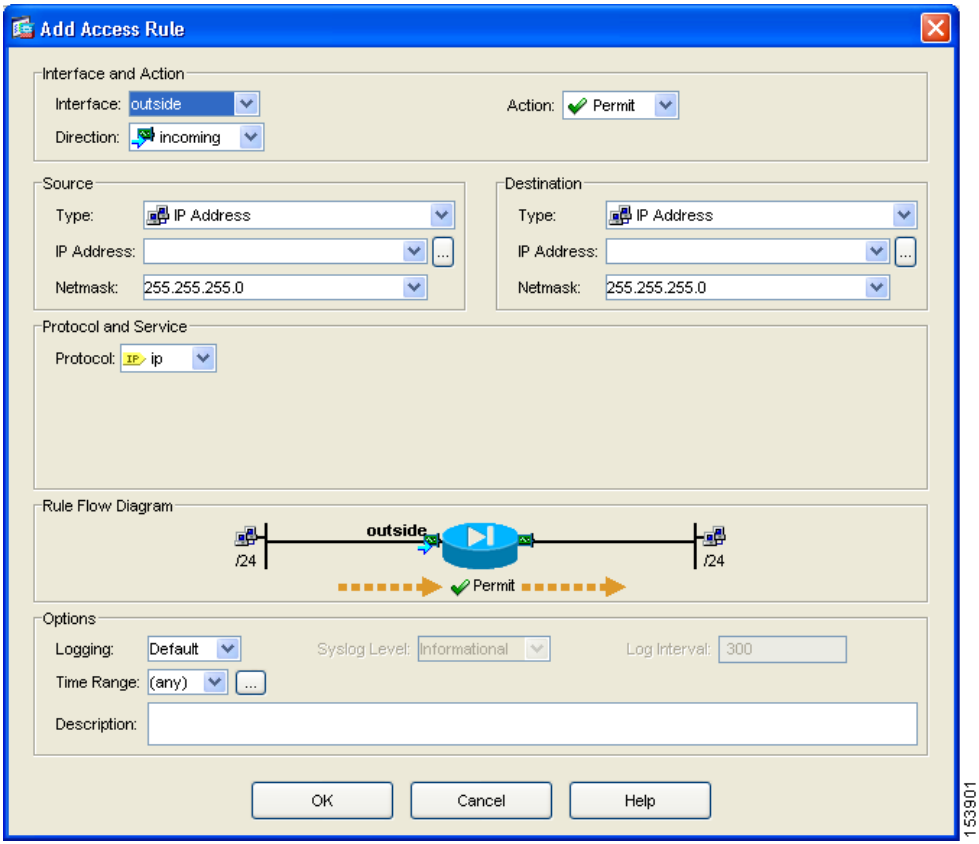
Step 1 In the ASDM window:

a. Click the **Configuration** tool.

b. In the Features pane, click **Security Policy**.

c. Click the **Access Rules** tab, and then from the Add pull-down list, choose Add Access Rule.

The Add Access Rule dialog box appears.



Step 2 In the Interface and Action area:

a. From the Interface drop-down list, choose Outside.

b. From the Direction drop-down list, choose Incoming.

c. From the Action drop-down list, choose Permit.

Step 3 In the Source area:

a. From the Type drop-down list, choose IP Address.

b. Enter the IP address of the source host or source network. Use 0.0.0.0 to allow traffic originating from any host or network.

Alternatively, if the address of the source host or network is preconfigured, choose the source IP address from the IP Address drop-down list.

c. Enter the netmask for the source IP address or select one from the Netmask drop-down list.

Step 4 In the Destination area:

a. In the IP address field, enter the public IP address of the destination host or network, such as a web server. (In this scenario, the public IP address of the DMZ web server is 209.165.200.226.)

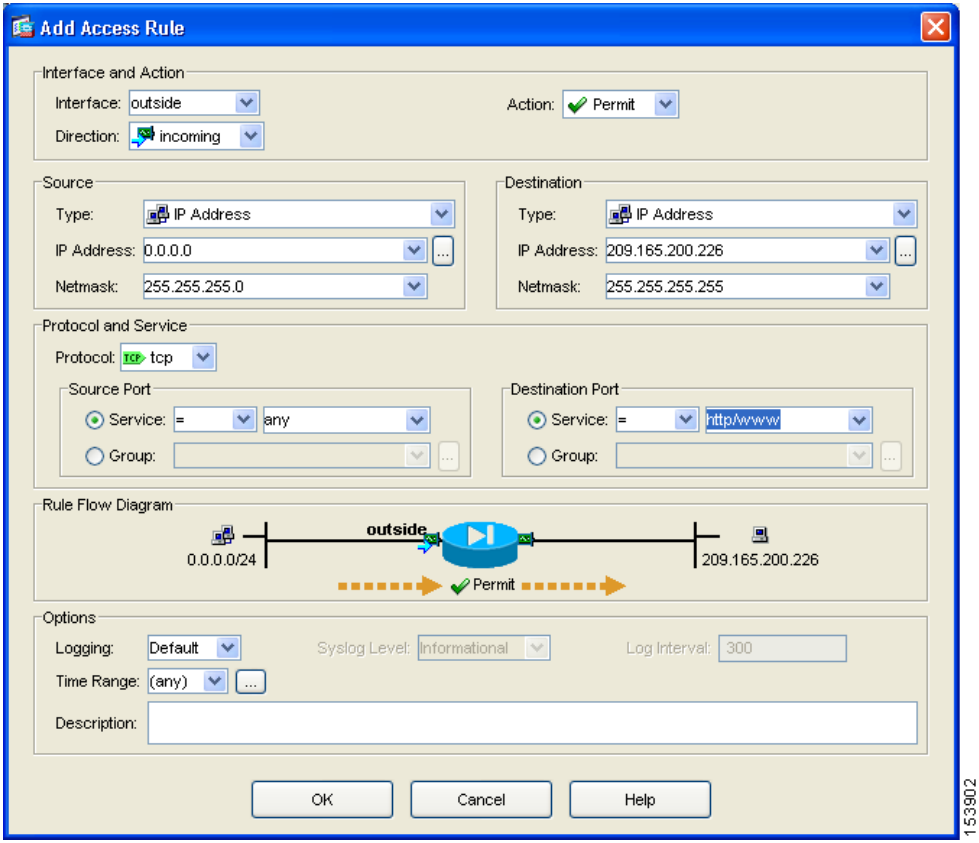
Step 5 In the Protocol and Service area, specify the type of traffic that you want to permit through the adaptive security appliance.

a. From the Protocol drop-down list, choose tcp.

b. In the Source Port area, click the **Service** radio button, choose "**=**" (equal to) from the Service drop-down list, and then choose Any from the next drop-down list.

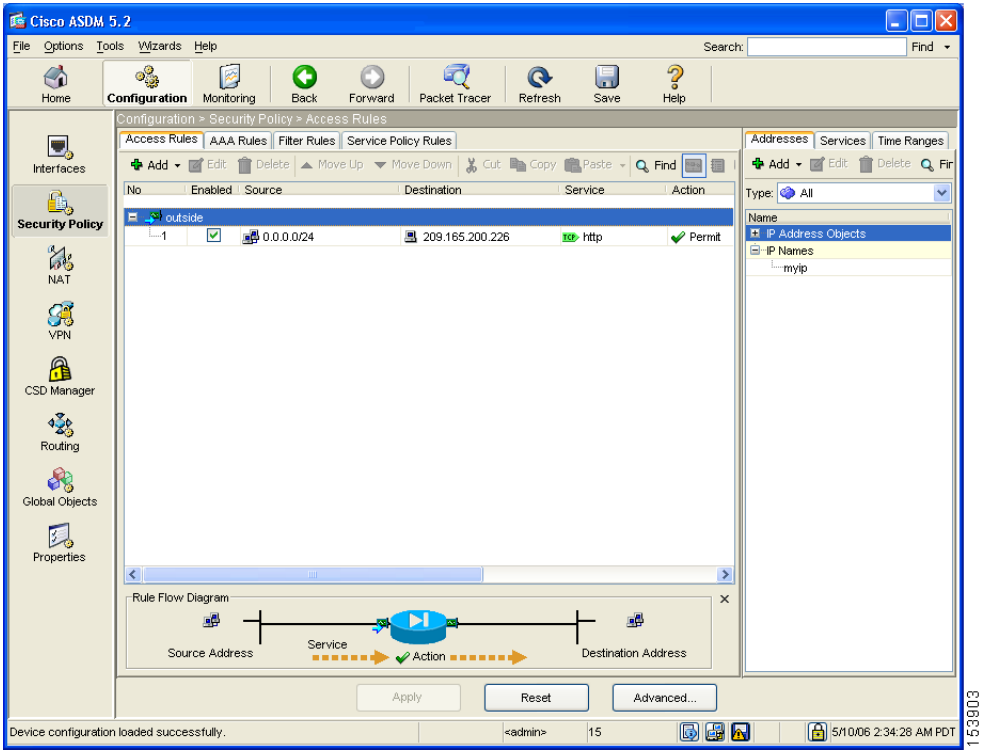
c. In the Destination Port area, click the **Service** radio button, choose "**=**" (equal to) from the Service drop-down list, and then choose HTTP/WWW from the next drop-down list.

At this point, the entries in the Add Access Rule dialog box should be similar to the following:



d. Click **OK**.

Step 6 The displayed configuration should be similar to the following. Verify that the information you entered is accurate.



Step 7 Click **Apply** to save the configuration changes to the configuration that the adaptive security appliance is currently running.

Clients on both the private and public networks can now resolve HTTP requests for content from the DMZ web server, while keeping the private network secure.

Note Although the destination address specified is the private address of the DMZ web server (10.30.30.30), HTTP traffic from any host on the Internet destined for the public address 209.165.200.226 is permitted through the adaptive security appliance. The address translation (209.165.200.226 to 10.30.30.30) allows the traffic to be permitted. For information about creating the translation rule, see the "Configuring NAT for Inside Clients to Communicate with the DMZ Web Server" section on page 6-12.

Step 8 If you want the configuration changes to be saved to the startup configuration so that they are applied the next time the device starts, from the File menu, click **Save**.

Alternatively, ASDM prompts you to save the configuration changes permanently when you exit ASDM.

If you do not save the configuration changes, the old configuration takes effect the next time the device starts.

What to Do Next

If you are deploying the adaptive security appliance solely to protect a web server in a DMZ, you have completed the initial configuration. You may want to consider performing some of the following additional steps:

To Do This ...	See ...
Refine configuration and configure optional and advanced features	*Cisco Security Appliance Command Line Configuration Guide*
Learn about daily operations	*Cisco Security Appliance Command Reference* *Cisco Security Appliance Logging Configuration and System Log Messages*
Review hardware maintenance and troubleshooting information	*Cisco ASA 5500 Series Hardware Installation Guide*

You can configure the adaptive security appliance for more than one application. The following sections provide configuration procedures for other common applications of the adaptive security appliance.

To Do This ...	See ...
Configure a remote-access VPN	Chapter 7, "Scenario: Remote-Access VPN Configuration"
Configure a site-to-site VPN	Chapter 8, "Scenario: Site-to-Site VPN Configuration"

Scenario: Remote-Access VPN Configuration

This chapter describes how to use the adaptive security appliance to accept remote-access IPsec VPN connections. A remote-access VPN enables you to create secure connections, or tunnels, across the Internet, thus providing secure access to off-site users.

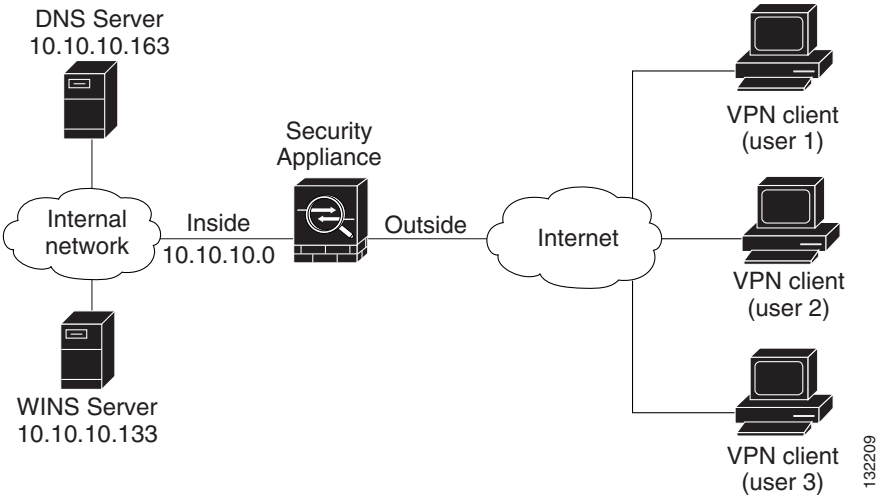
If you are implementing an Easy VPN solution, this chapter describes how to configure the Easy VPN server (sometimes called a headend device).

This chapter includes the following sections:

Example IPsec Remote-Access VPN Network Topology

Figure 7-1 shows an adaptive security appliance configured to accept requests from and establish IPsec connections with VPN clients, such as a Cisco Easy VPN hardware client, over the Internet.

Figure 7-1 Network Layout for Remote Access VPN Scenario



Implementing the IPsec Remote-Access VPN Scenario

This section describes how to configure the adaptive security appliance to accept IPsec VPN connections from remote clients and devices. If you are implementing an Easy VPN solution, this section describes how to configure an Easy VPN server (also known as a headend device).

Values for example configuration settings are taken from the remote-access scenario illustrated in Figure 7-1.

This section includes the following topics:

Information to Have Available

Before you begin configuring the adaptive security appliance to accept remote access IPsec VPN connections, make sure that you have the following information available:

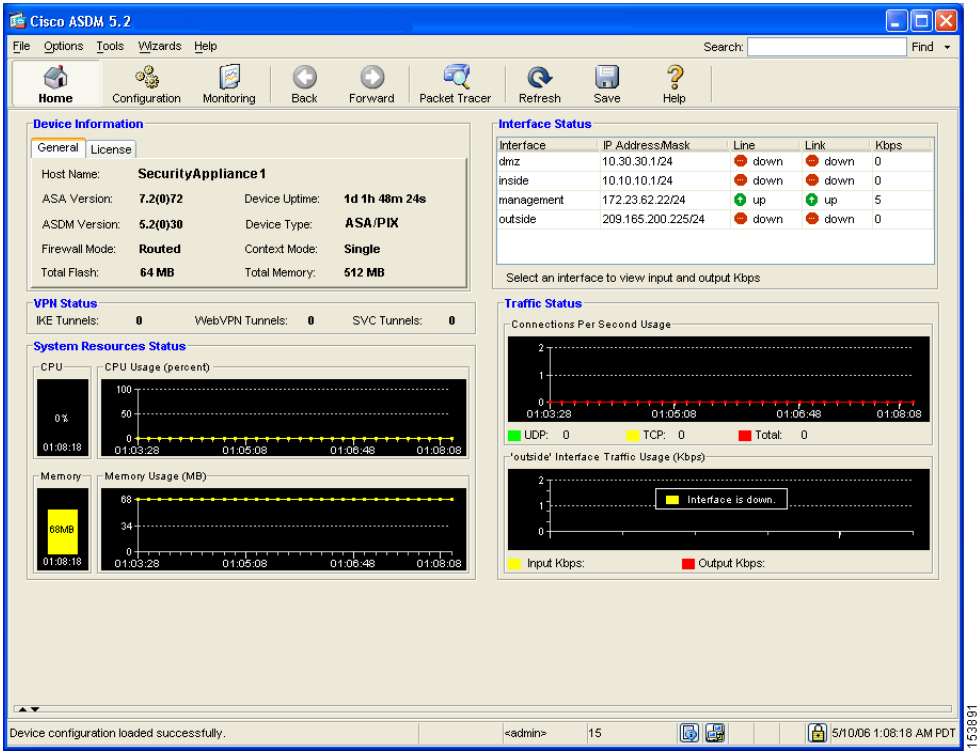
- Range of IP addresses to be used in an IP pool. These addresses are assigned to remote VPN clients as they are successfully connected.
- List of users to be used in creating a local authentication database, unless you are using a AAA server for authentication.
- Networking information to be used by remote clients when connecting to the VPN, including:
  - IP addresses for the primary and secondary DNS servers
  - IP addresses for the primary and secondary WINS servers
  - Default domain name
  - List of IP addresses for local hosts, groups, and networks that should be made accessible to authenticated remote clients

Starting ASDM

To run ASDM in a web browser, enter the factory default IP address in the address field: **https://192.168.1.1/admin/**.

Note Remember to add the "**s**" in "**https**" or the connection fails. HTTPS (HTTP over SSL) provides a secure connection between your browser and the adaptive security appliance.

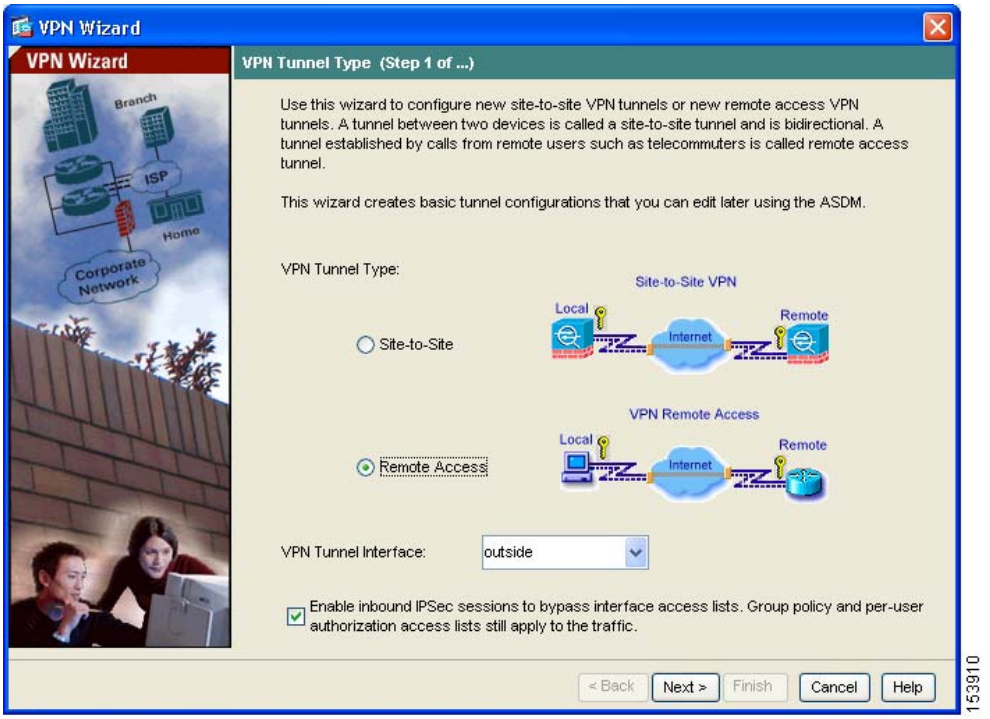
The Main ASDM window appears.



Configuring the FWSM for an IPsec Remote-Access VPN

To begin the process for configuring a remote-access VPN, perform the following steps:

Step 1 In the main ASDM window, choose **VPN Wizard** from the Wizards drop-down menu. The VPN Wizard Step 1 screen appears.



Step 2 In Step 1 of the VPN Wizard, perform the following steps:

a. Click the **Remote Access VPN** radio button.

b. From the drop-down list, choose Outside as the enabled interface for the incoming VPN tunnels.

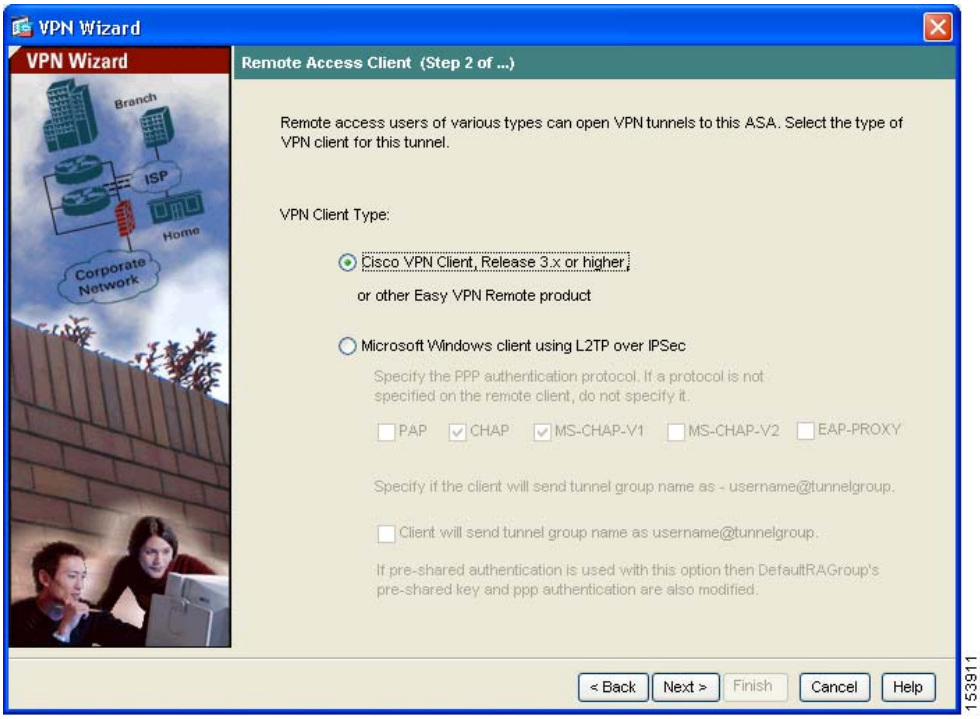
c. Click **Next** to continue.

Selecting VPN Client Types

In Step 2 of the VPN Wizard, perform the following steps:

Step 1 Specify the type of VPN client that will enable remote users to connect to this adaptive security appliance. For this scenario, click the **Cisco VPN Client** radio button.

You can also use any other Cisco Easy VPN remote product.



Step 2 Click **Next** to continue.

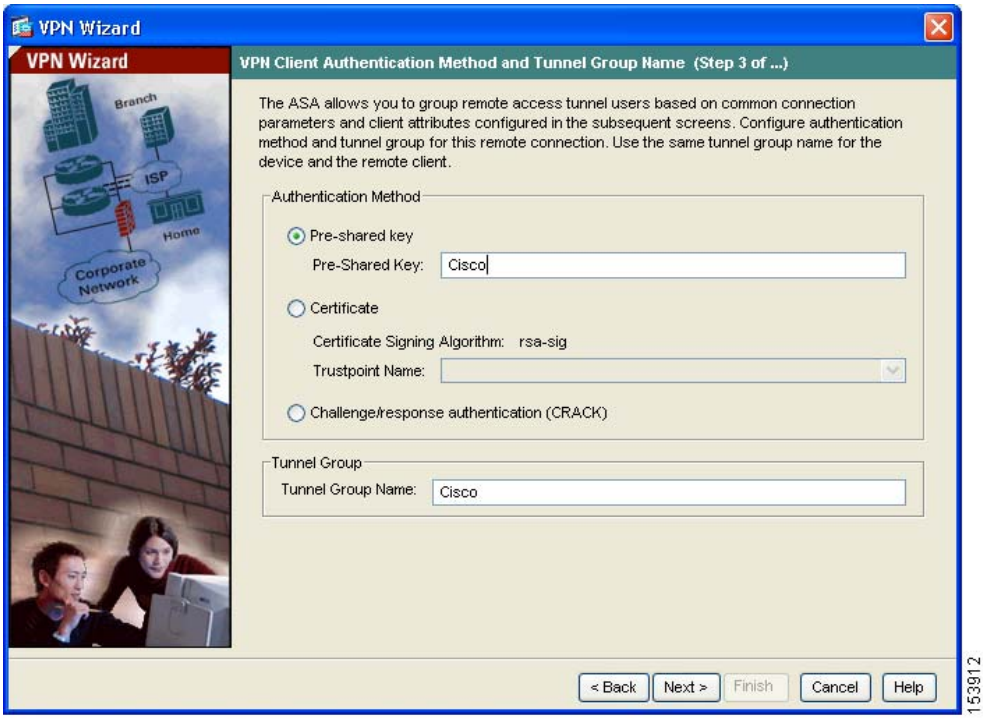
Specifying the VPN Tunnel Group Name and Authentication Method

In Step 3 of the VPN Wizard, perform the following steps:

Step 1 Specify the type of authentication that you want to use by performing one of the following steps:

- To use a static preshared key for authentication, click the **Pre-Shared Key** radio button and enter a preshared key (for example, “Cisco”). This key is used for IPsec negotiations between the adaptive security appliances.
- To use digital certificates for authentication, click the **Certificate** radio button, choose the Certificate Signing Algorithm from the drop-down list, and then choose a pre-configured trustpoint name from the drop-down list.

  If you want to use digital certificates for authentication but have not yet configured a trustpoint name, you can continue with the Wizard by using one of the other two options. You can revise the authentication configuration later using the standard ASDM screens.
- Click the **Challenge/Response Authentication (CRACK)** radio button to use that method of authentication.



Step 2 Enter a Tunnel Group Name (such as “Cisco”) for the set of users that use common connection parameters and client attributes to connect to this adaptive security appliance.

Step 3 Click **Next** to continue.

Specifying a User Authentication Method

Users can be authenticated either by a local authentication database or by using external authentication, authorization, and accounting (AAA) servers (RADIUS, TACACS+, SDI, NT, Kerberos, and LDAP).

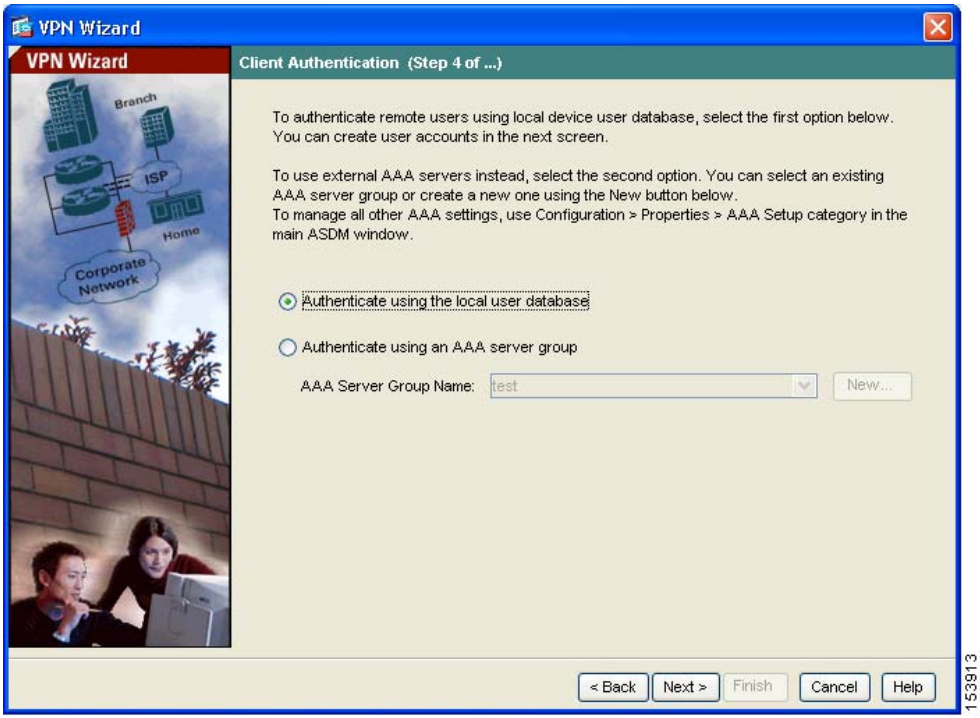
In Step 4 of the VPN Wizard, perform the following steps:

Step 1 If you want to authenticate users by creating a user database on the adaptive security appliance, click the **Authenticate Using the Local User Database** radio button.

Step 2 If you want to authenticate users with an external AAA server group:

a. Click the **Authenticate Using an AAA Server Group** radio button.

b. Choose a preconfigured server group from the drop-down list, or click **New** to add a new server group.



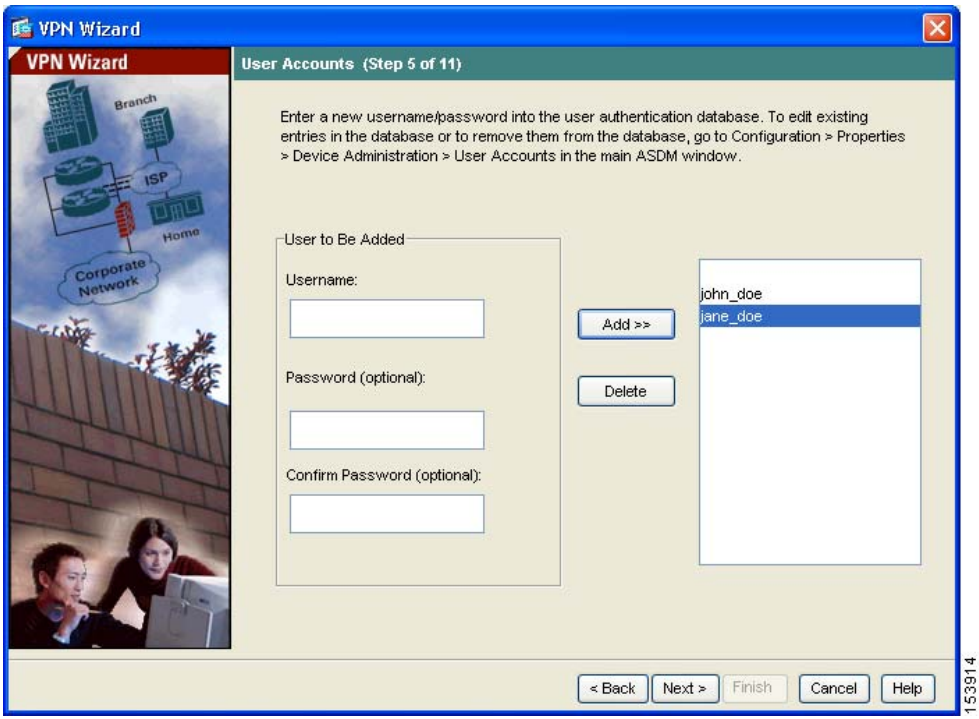
Step 3 Click **Next** to continue.

(Optional) Configuring User Accounts

If you have chosen to authenticate users with the local user database, you can create new user accounts here. You can also add users later using the ASDM configuration interface.

In Step 5 of the VPN Wizard, perform the following steps:

Step 1 To add a new user, enter a username and password, and then click **Add**.



Step 2 When you have finished adding new users, click **Next** to continue.

Configuring Address Pools

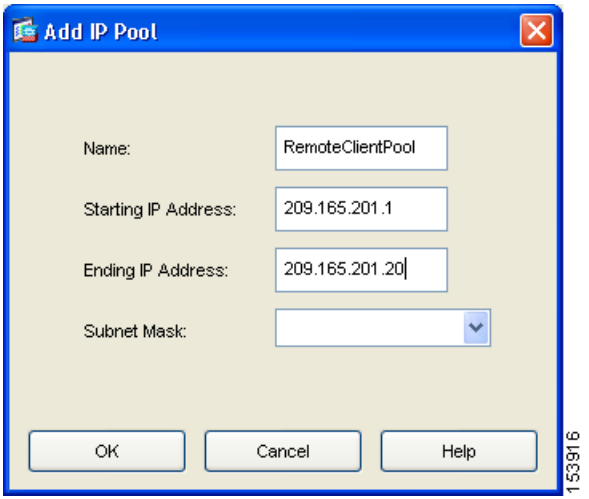
For remote clients to gain access to your network, you must configure a pool of IP addresses that can be assigned to remote VPN clients as they are successfully connected. In this scenario, the pool is configured to use the range of IP addresses 209.165.201.1–209.166.201.20.

In Step 6 of the VPN Wizard, perform the following steps:

Step 1 Enter a pool name or choose a preconfigured pool from the drop-down list.

Alternatively, click **New** to create a new address pool.

The Add IP Pool dialog box appears.

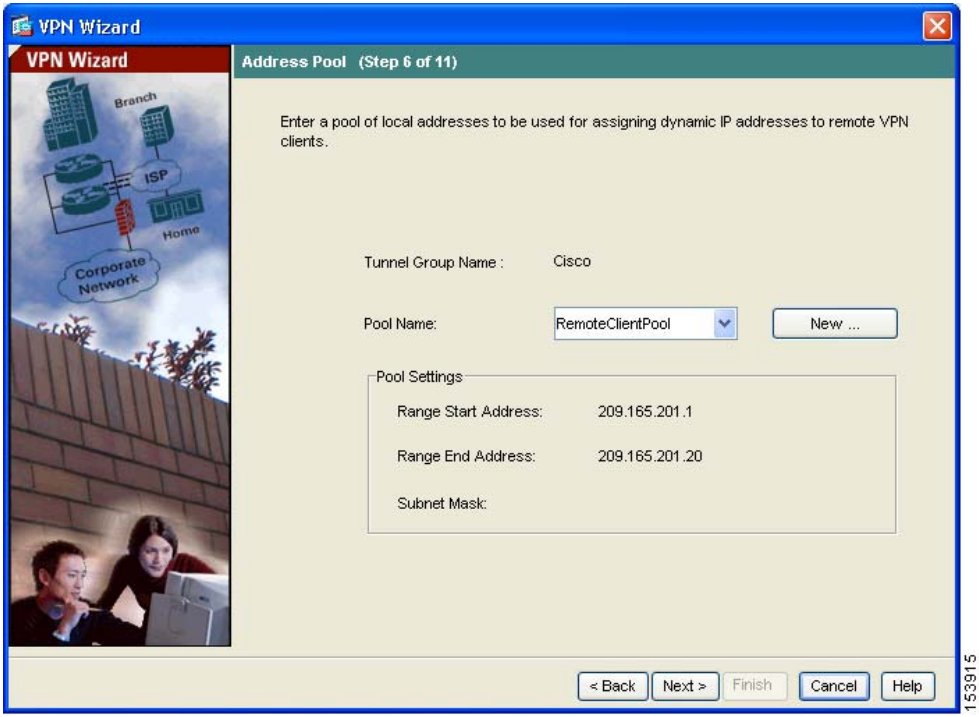


Step 2 In the Add IP Pool dialog box:

a. Enter the Starting IP address and Ending IP address of the range.

b. (Optional) Enter the Netmask for the range of IP addresses.

c. Click **OK** to return to Step 6 of the VPN Wizard.



Step 3 Click **Next** to continue.

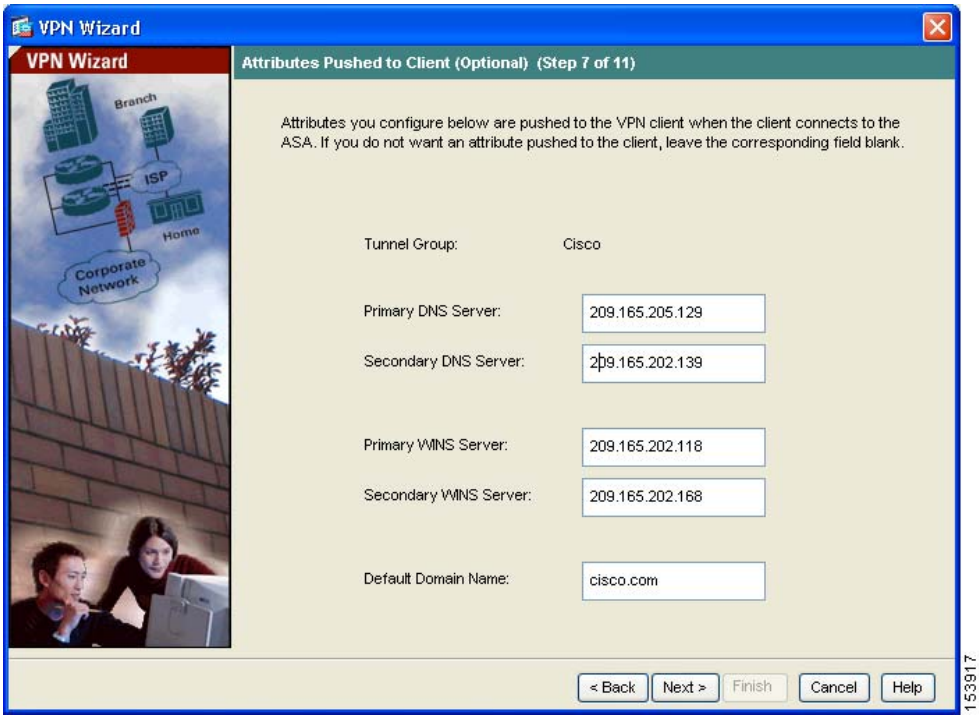
Configuring Client Attributes

To access your network, each remote access client needs basic network configuration information, such as which DNS and WINS servers to use and the default domain name. Rather than configuring each remote client individually, you can provide the client information to ASDM. The adaptive security appliance pushes this information to the remote client or Easy VPN hardware client when a connection is established.

Ensure that you specify the correct values, or remote clients will not be able to use DNS names for resolution or use Windows networking.

In Step 7 of the VPN Wizard, perform the following steps:

Step 1 Enter the network configuration information to be pushed to remote clients.



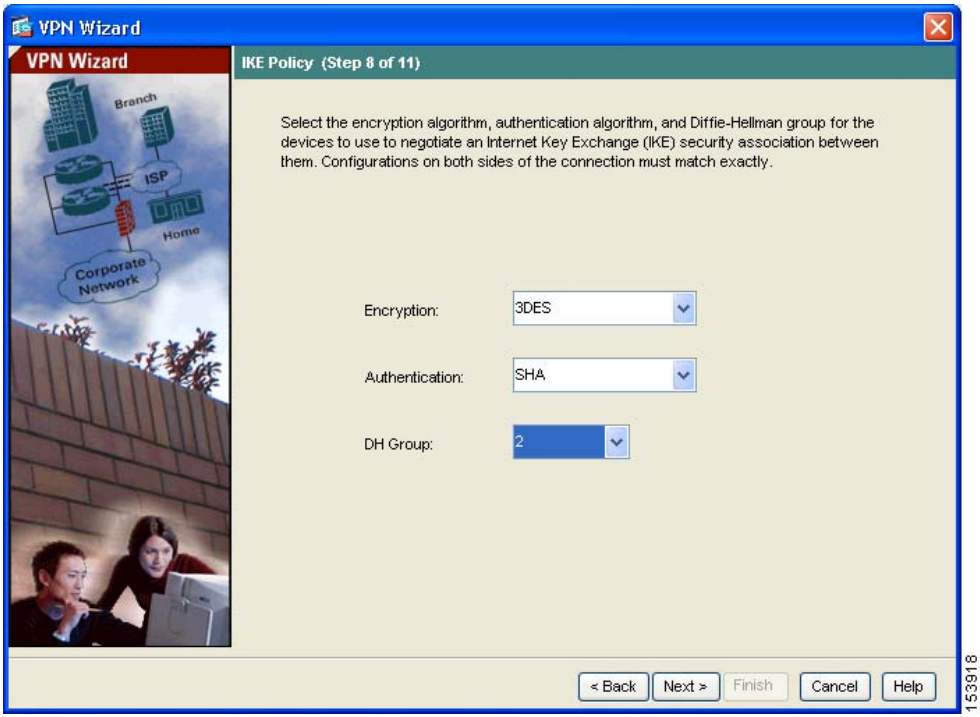
Step 2 Click **Next** to continue.

Configuring the IKE Policy

IKE is a negotiation protocol that includes an encryption method to protect data and ensure privacy; it is also an authentication method to ensure the identity of the peers. In most cases, the ASDM default values are sufficient to establish secure VPN tunnels.

To specify the IKE policy in Step 8 of the VPN Wizard, perform the following steps:

Step 1 Click the Encryption (DES/3DES/AES), authentication algorithms (MD5/SHA), and the Diffie-Hellman group (1/2/5/7) used by the adaptive security appliance during an IKE security association.

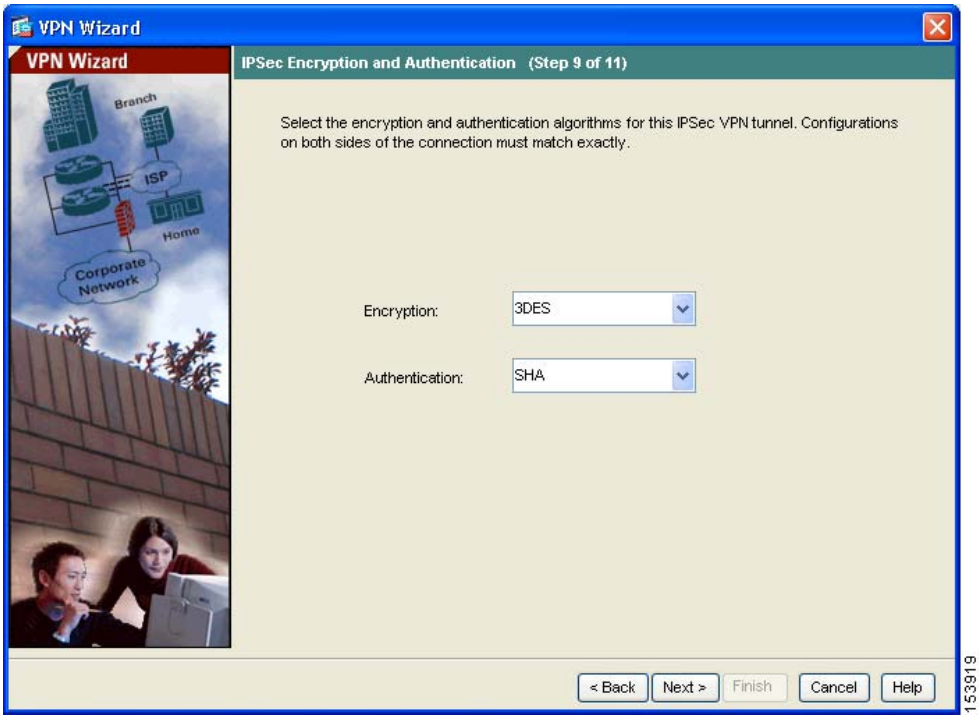


Step 2 Click **Next** to continue.

Configuring IPsec Encryption and Authentication Parameters

In Step 9 of the VPN Wizard, perform the following steps:

Step 1 Click the Encryption algorithm (DES/3DES/AES) and authentication algorithm (MD5/SHA).



Step 2 Click **Next** to continue.

Specifying Address Translation Exception and Split Tunneling

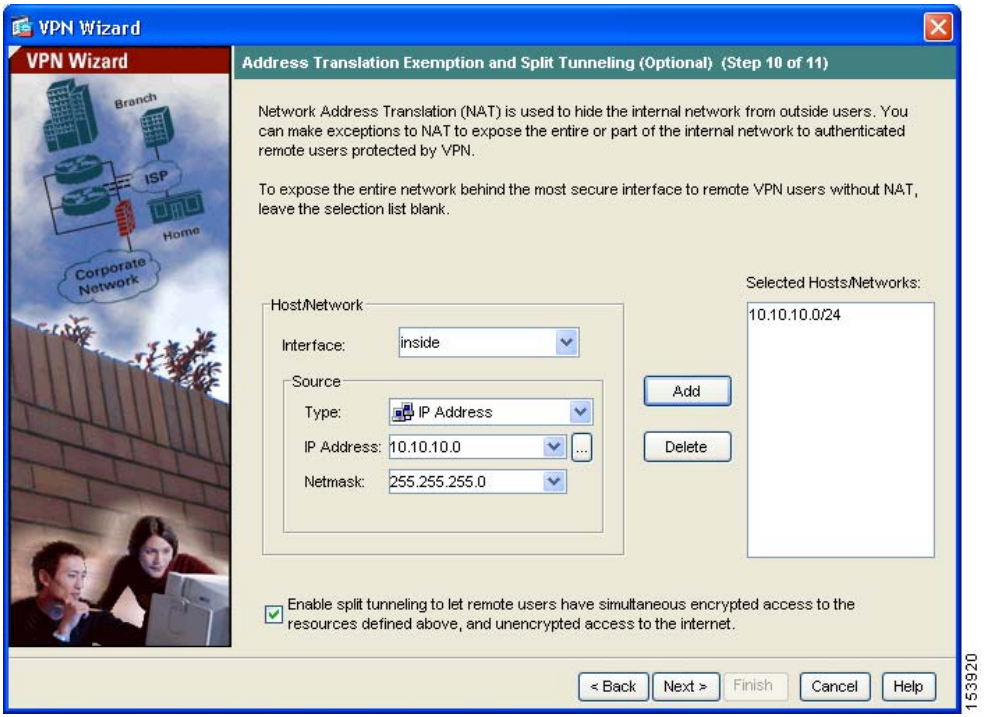
Split tunneling lets a remote-access IPsec client conditionally direct packets over an IPsec tunnel in encrypted form or to a network interface in clear text form.

The adaptive security appliance uses Network Address Translation (NAT) to prevent internal IP addresses from being exposed externally. You can make exceptions to this network protection by identifying local hosts and networks that should be made accessible to authenticated remote users. (In this scenario, the entire inside network 10.10.10.0 is exposed to all remote clients.)

In Step 10 of the VPN Wizard, perform the following steps:

Step 1 Specify hosts, groups, and networks that should be in the list of internal resources made accessible to authenticated remote users.

To add or remove hosts, groups, and networks dynamically from the Selected Hosts/Networks pane, click **Add** or **Delete**, respectively.

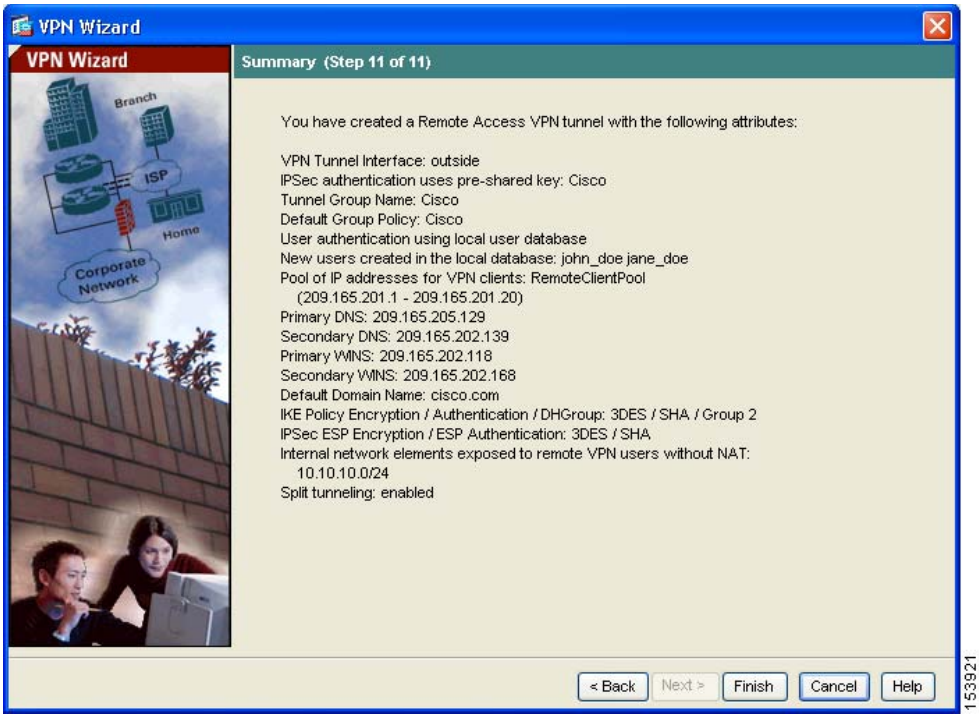


Note Enable split tunneling by checking the **Enable Split Tunneling** check box at the bottom of the screen. Split tunneling allows traffic outside the configured networks to be sent out directly to the Internet instead of over the encrypted VPN tunnel.

Step 2 Click **Next** to continue.

Verifying the Remote-Access VPN Configuration

In Step 11 of the VPN Wizard, review the configuration attributes for the VPN tunnel you just created. The displayed configuration should be similar to the following:



If you are satisfied with the configuration, click **Finish** to apply the changes to the adaptive security appliance.

If you want the configuration changes to be saved to the startup configuration so that they are applied the next time the device starts, from the File menu, click **Save**. Alternatively, ASDM prompts you to save the configuration changes permanently when you exit ASDM.

If you do not save the configuration changes, the old configuration takes effect the next time the device starts.

What to Do Next

If you are deploying the adaptive security appliance solely in a remote-access VPN environment, you have completed the initial configuration. In addition, you may want to consider performing some of the following steps:

To Do This ...	See ...
Refine configuration and configure optional and advanced features	*Cisco Security Appliance Command Line Configuration Guide*
Learn about daily operations	*Cisco Security Appliance Command Reference* *Cisco Security Appliance Logging Configuration and System Log Messages*
Review hardware maintenance and troubleshooting information	*Cisco ASA 5500 Series Hardware Installation Guide*

You can configure the adaptive security appliance for more than one application. The following sections provide configuration procedures for other common applications of the adaptive security appliance.

To Do This ...	See ...
Configure the adaptive security appliance to protect a Web server in a DMZ	Chapter 6, "Scenario: DMZ Configuration"
Configure a site-to-site VPN	Chapter 8, "Scenario: Site-to-Site VPN Configuration"

Scenario: Site-to-Site VPN Configuration

This chapter describes how to use the adaptive security appliance to create a site-to-site VPN.

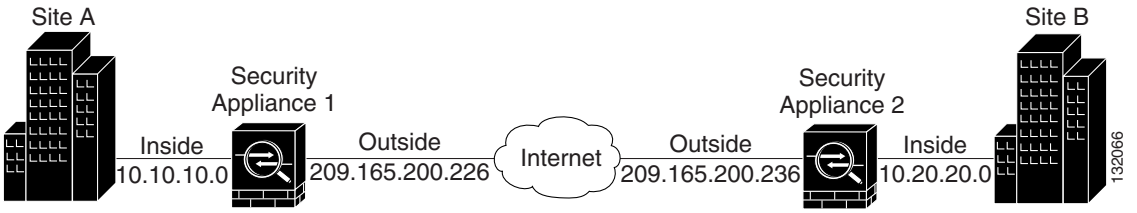
Site-to-site VPN features provided by the adaptive security appliance enable businesses to extend their networks across low-cost public Internet connections to business partners and remote offices worldwide while maintaining their network security. A VPN connection enables you to send data from one location to another over a secure connection, or tunnel, first by authenticating both ends of the connection, and then by automatically encrypting all data sent between the two sites.

This chapter includes the following sections:

Example Site-to-Site VPN Network Topology

Figure 8-1 shows an example VPN tunnel between two adaptive security appliances.

Figure 8-1 Network Layout for Site-to-Site VPN Configuration Scenario



Creating a VPN site-to-site deployment such as the one in Figure 8-1 requires you to configure two adaptive security appliances, one on each side of the connection.

Implementing the Site-to-Site Scenario

This section describes how to configure the adaptive security appliance in a site-to-site VPN deployment, using example parameters from the remote-access scenario shown in Figure 8-1.

This section includes the following sections:

Information to Have Available

Before you begin the configuration procedure, gather the following information:

- IP address of the remote adaptive security appliance peer
- IP addresses of local hosts and networks permitted to use the tunnel to communicate with resources on the remote site
- IP addresses of remote hosts and networks permitted to use the tunnel to communicate with local resources

Configuring the Site-to-Site VPN

This section describes how to use the ASDM VPN Wizard to configure the adaptive security appliance for a site-to-site VPN.

This section includes the following topics:

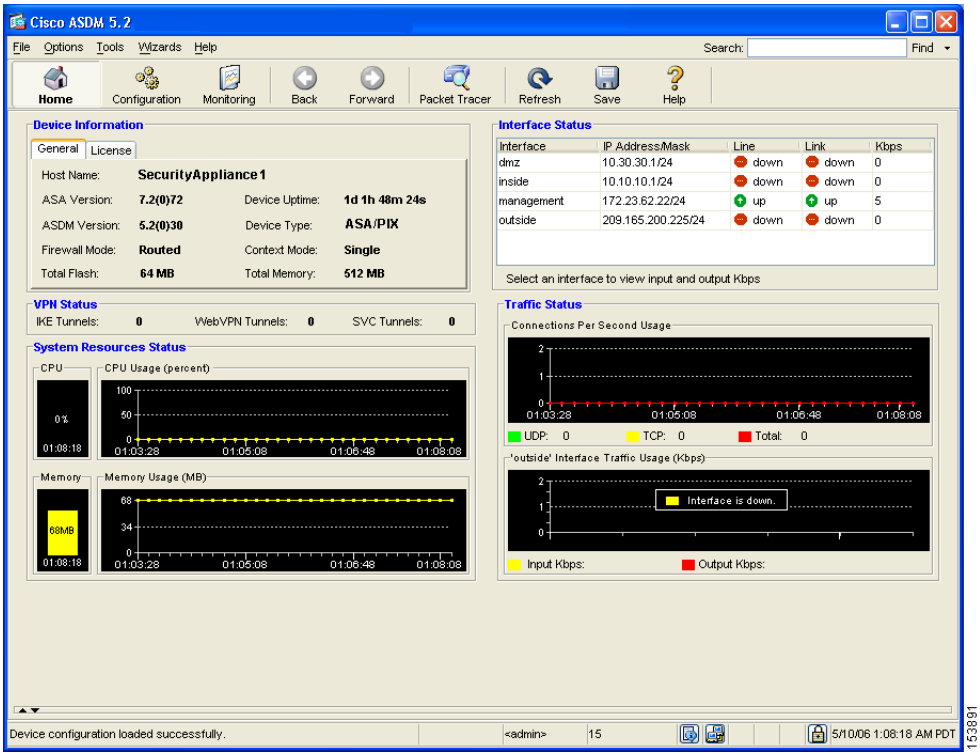
The following sections provide detailed instructions for how to perform each configuration step.

Starting ASDM

To run ASDM in a web browser, enter the factory default IP address in the address field: **https://192.168.1.1/admin/**.

Note Remember to add the "**s**" in "**https**" or the connection fails. HTTPS (HTTP over SSL) provides a secure connection between your browser and the adaptive security appliance.

The Main ASDM window appears.



Configuring the Security Appliance at the Local Site

Note The adaptive security appliance at the first site is referred to as Security Appliance 1 from this point forward.

To configure the Security Appliance 1, perform the following steps:

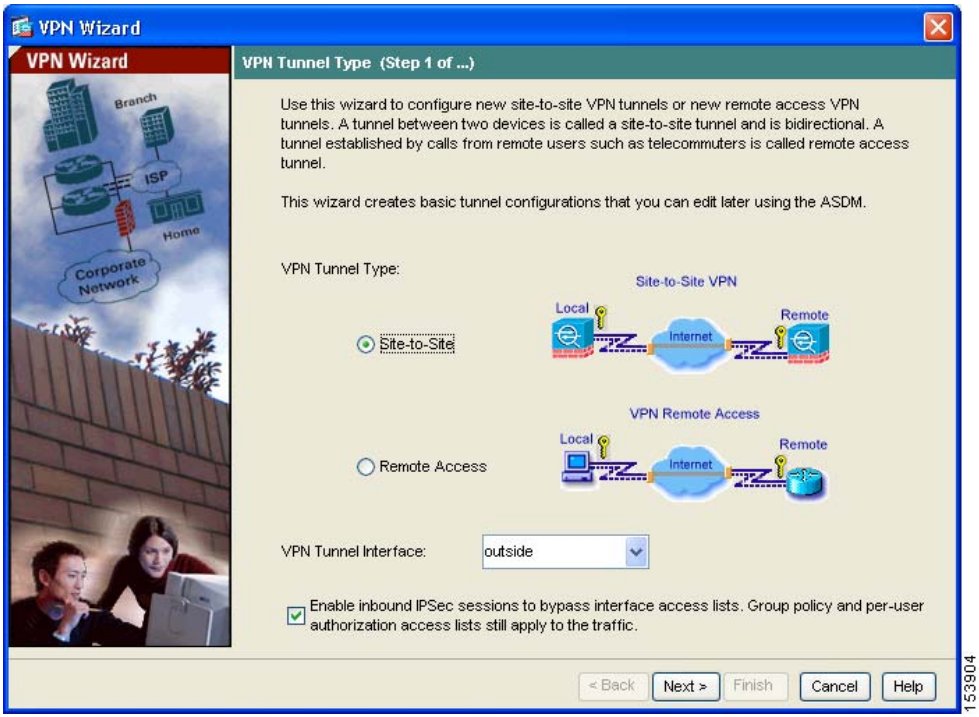
Step 1 In the main ASDM window, choose the VPN Wizard option from the Wizards drop-down menu. ASDM opens the first VPN Wizard screen.

In Step 1 of the VPN Wizard, perform the following steps:

a. Click the **Site-to-Site VPN** radio button.

Note The Site-to-Site VPN option connects two IPSec security gateways, which can include adaptive security appliances, VPN concentrators, or other devices that support site-to-site IPSec connectivity.

b. From the drop-down list, choose Outside as the enabled interface for the current VPN tunnel.



c. Click **Next** to continue.

Providing Information About the Remote VPN Peer

The VPN peer is the system on the other end of the connection that you are configuring, usually at a remote site.

Note In this scenario, the remote VPN peer is referred to as Security Appliance 2 from this point forward.

In Step 2 of the VPN Wizard, perform the following steps:

Step 1 Enter the Peer IP Address (the IP address of Security Appliance 2, in this scenario 209.165.200.236) and a Tunnel Group Name (for example "Cisco").

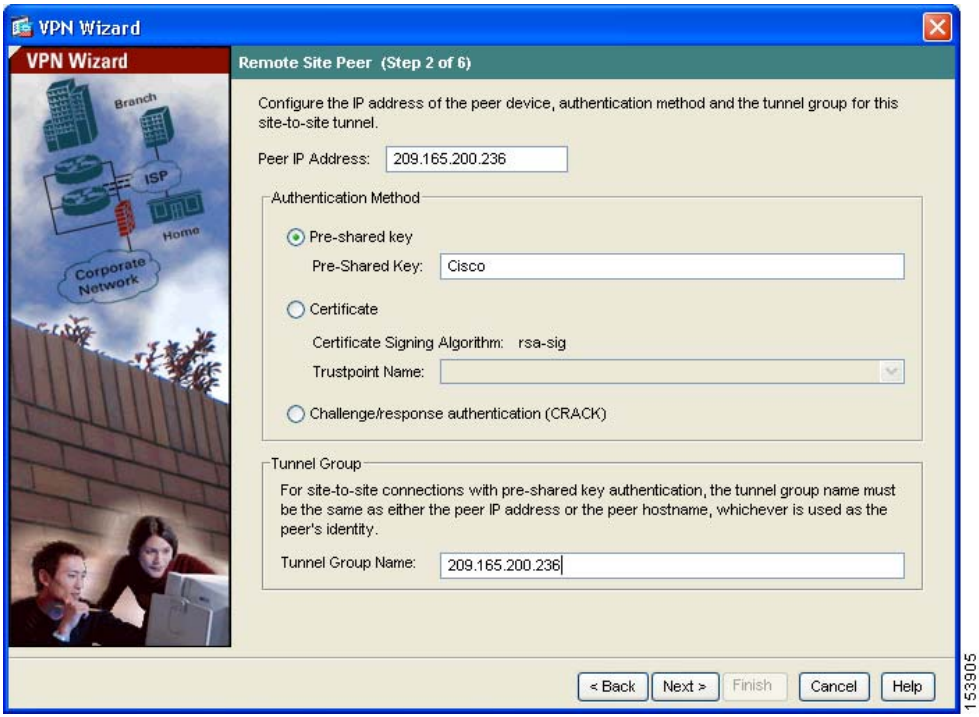
Step 2 Specify the type of authentication that you want to use by performing one of the following steps:

- To use a static preshared key for authentication, click the **Pre-Shared Key** radio button and enter a preshared key (for example, "Cisco"). This key is used for IPSec negotiations between the adaptive security appliances.

  Note When you configure Security Appliance 2 at the remote site, the VPN peer is Security Appliance 1. Be sure to enter the same preshared key (Cisco) that you use here.

- Click the **Challenge/Response Authentication** radio button to use that method of authentication.
- To use digital certificates for authentication, click the **Certificate** radio button, choose the Certificate Signing Algorithm from the drop-down list, and then choose a preconfigured trustpoint name from the drop-down list.

  If you want to use digital certificates for authentication but have not yet configured a trustpoint name, you can continue with the Wizard by using one of the other two options. You can revise the authentication configuration later using the standard ASDM screens.



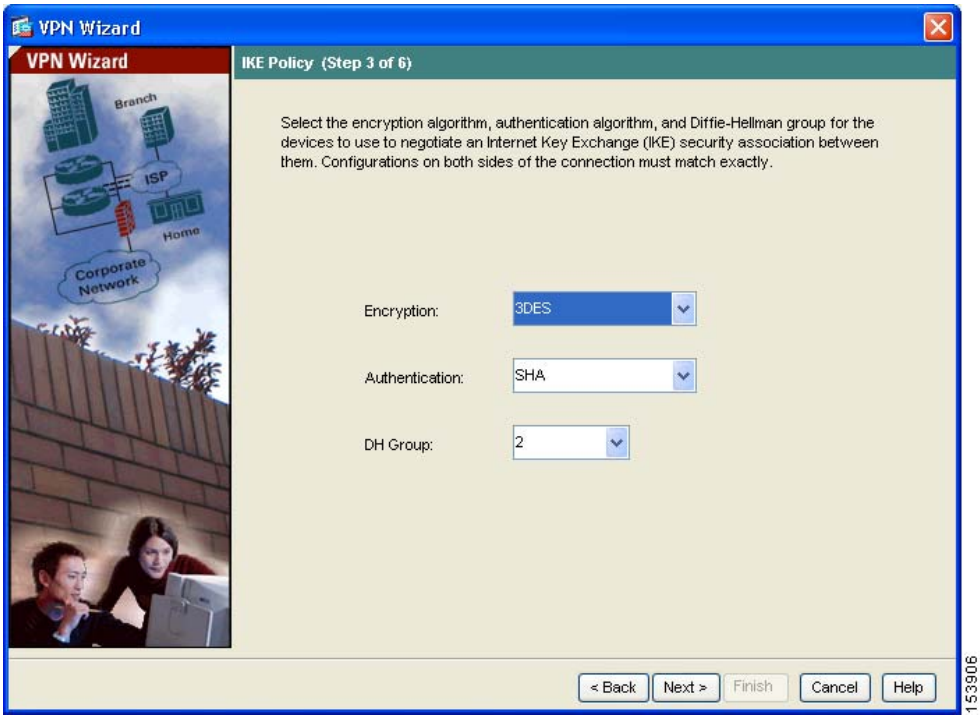
Step 3 Click **Next** to continue.

Configuring the IKE Policy

IKE is a negotiation protocol that includes an encryption method to protect data and ensure privacy; it is also an authentication method to ensure the identity of the peers. In most cases, the ASDM default values are sufficient to establish secure VPN tunnels between two peers.

In Step 3 of the VPN Wizard, perform the following steps:

Step 1 Click the Encryption (DES/3DES/AES), authentication algorithms (MD5/SHA), and the Diffie-Hellman group (1/2/5) used by the adaptive security appliance during an IKE security association.



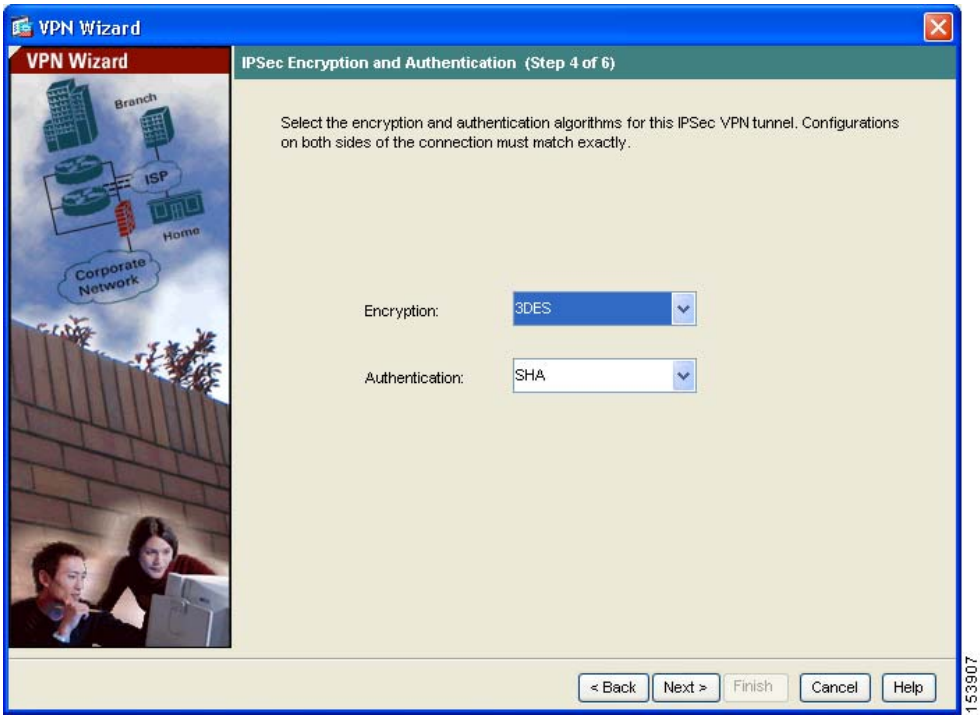
Note When configuring Security Appliance 2, enter the exact values for each of the options that you chose for Security Appliance 1. Encryption mismatches are a common cause of VPN tunnel failures and can slow down the process.

Step 2 Click **Next** to continue.

Configuring IPSec Encryption and Authentication Parameters

In Step 4 of the VPN Wizard, perform the following steps:

Step 1 Choose the Encryption algorithm (DES/3DES/AES) and authentication algorithm (MD5/SHA) from the drop-down lists.



Step 2 Click **Next** to continue.

Specifying Hosts and Networks

Identify hosts and networks at the local site that are permitted to use this IPSec tunnel to communicate with the remote-site peer. Add or remove hosts and networks dynamically by clicking **Add** or **Delete**, respectively. In the current scenario, traffic from Network A (10.10.10.0) is encrypted by Security Appliance 1 and transmitted through the VPN tunnel.

In addition, identify hosts and networks at the remote site to be allowed to use this IPSec tunnel to access local hosts and networks. Add or remove hosts and networks dynamically by clicking **Add** or **Delete** respectively. In this scenario, for Security Appliance 1, the remote network is Network B (10.20.20.0), so traffic encrypted from this network is permitted through the tunnel.

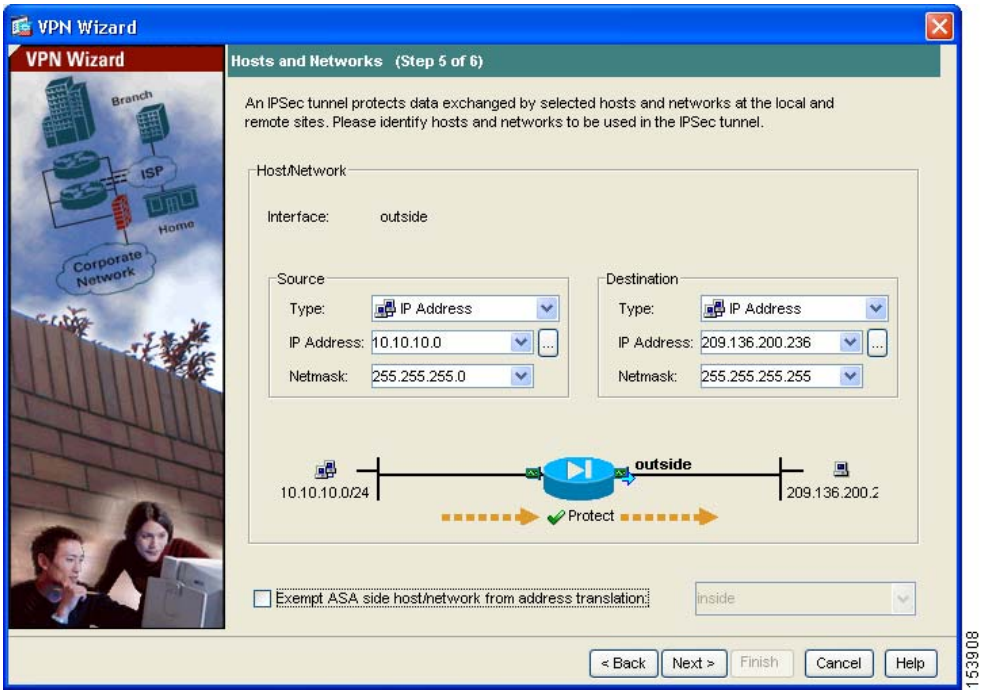
In Step 5 of the VPN Wizard, perform the following steps:

Step 1 In the Source area, choose IP Address from the Type drop-down list.

Step 2 Enter the local IP address and netmask in the IP Address and Netmask fields.

Step 3 In the Destination area, choose IP Address from the Type drop-down list.

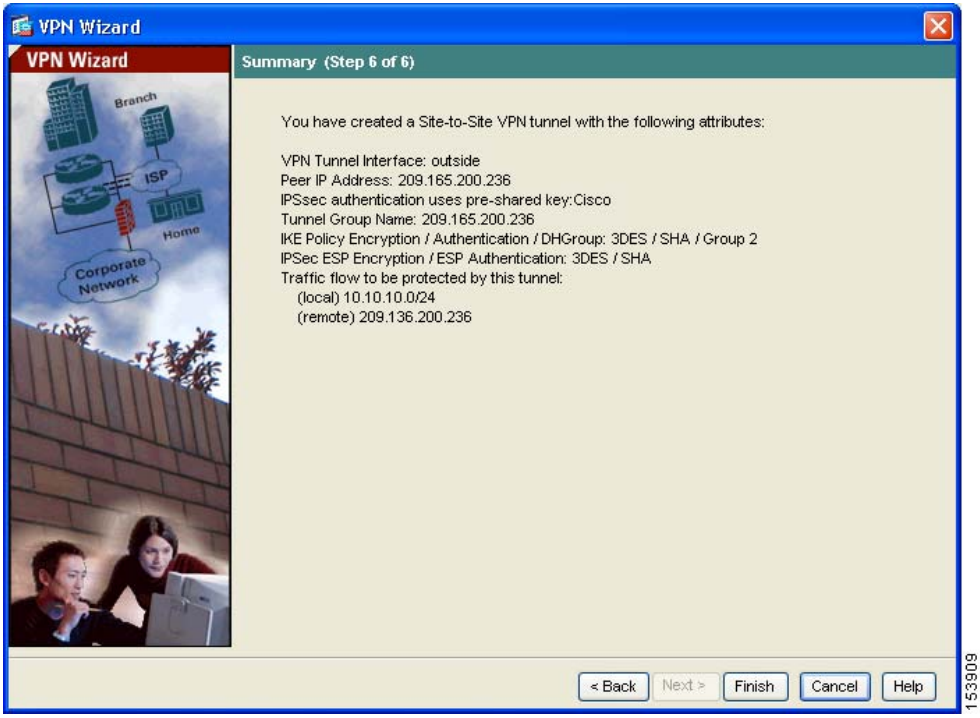
Step 4 Enter the IP address and Netmask for the remote host or network.



Step 5 Click **Next** to continue.

Viewing VPN Attributes and Completing the Wizard

In Step 6 of the VPN Wizard, review the configuration list for the VPN tunnel you just created. If you are satisfied with the configuration, click **Finish** to apply the changes to the adaptive security appliance.



If you want the configuration changes to be saved to the startup configuration so that they are applied the next time the device starts, from the File menu, click **Save**.

Alternatively, ASDM prompts you to save the configuration changes permanently when you exit ASDM.

If you do not save the configuration changes, the old configuration takes effect the next time the device starts.

This concludes the configuration process for Security Appliance 1.

Configuring the Other Side of the VPN Connection

You have just configured the local adaptive security appliance. Now you need to configure the adaptive security appliance at the remote site.

At the remote site, configure the second adaptive security appliance to serve as a VPN peer. Use the procedure you used to configure the local adaptive security appliance, starting with the "Configuring the Security Appliance at the Local Site" section on page 8-4 and finishing with the "Viewing VPN Attributes and Completing the Wizard" section on page 8-11.

Note When configuring Security Appliance 2, enter the exact same values for each of the options that you selected for Security Appliance 1. Mismatches are a common cause of VPN configuration failures.

What to Do Next

If you are deploying the adaptive security appliance solely in a site-to-site VPN environment, you have completed the initial configuration. In addition, you may want to consider performing some of the following steps:

To Do This ...	See ...
Refine configuration and configure optional and advanced features	*Cisco Security Appliance Command Line Configuration Guide*
Learn about daily operations	*Cisco Security Appliance Command Reference* *Cisco Security Appliance Logging Configuration and System Log Messages*
Review hardware maintenance and troubleshooting information	*Cisco ASA 5500 Series Hardware Installation Guide*

You can configure the adaptive security appliance for more than one application. The following sections provide configuration procedures for other common applications of the adaptive security appliance.

To Do This ...	See ...
Configure the adaptive security appliance to protect a web server in a DMZ	Chapter 6, "Scenario: DMZ Configuration"
Configure a remote-access VPN	Chapter 7, "Scenario: Remote-Access VPN Configuration"

Configuring the AIP SSM

The optional AIP SSM runs advanced IPS software that provides further security inspection either in inline mode or promiscuous mode. The adaptive security appliance diverts packets to the AIP SSM just before the packet exits the egress interface (or before VPN encryption occurs, if configured) and after other firewall policies are applied. For example, packets that are blocked by an access list are not forwarded to the AIP SSM.

If you purchased an AIP SSM, use the procedures in this chapter to:

- Configure the adaptive security appliance to identify traffic to be diverted to the AIP SSM
- Session in to the AIP SSM and run setup

Note The AIP SSM is supported in ASA software versions 7.01 and later.

This chapter includes the following sections:

AIP SSM Configuration

This procedure describes the configuration steps you must take to configure the adaptive security appliance for AIP SSM.

This section includes the following topics:

Overview of Configuration Process

Configuring the AIP SSM is a three-part process that involves configuration of the adaptive security appliance first, then configuration of the AIP SSM, and then the configuration of the IPS software:

1. On the ASA 5500 series adaptive security appliance, identify traffic to divert to the AIP SSM (as described in the "Configuring the ASA 5500 to Divert Traffic to the AIP SSM" section on page 9-2).
2. On the AIP SSM, configure the inspection and protection policy, which determines how to inspect traffic and what to do when an intrusion is detected.
3. Configure the IPS software that runs on the AIP SSM. Information about the IPS software is beyond the scope of this document. Detailed information about IPS software configuration is available in the following separate documentation that came with your IPS product:
   - *Configuring the Cisco Intrusion Prevention System Sensor Using the Command Line Interface*
   - *Cisco Intrusion Prevention System Command Reference*

Configuring the ASA 5500 to Divert Traffic to the AIP SSM

You use MPF (Modular Policy Framework) commands to configure the adaptive security appliance to divert traffic to the AIP SSM. This procedure provides sufficient information to configure a simple set of policies in an AIP SSM deployment. If you want to create a more complex set of policies, read the Modular Policy Framework chapter in *Cisco Security Appliance Command Line Configuration Guide* which introduces Modular Policy Framework concepts and common commands.

To identify traffic to divert from the adaptive security appliance to the AIP SSM, perform the following steps:

Step 1 Create an access list that matches all traffic:

```
hostname(config)# access-list acl-name permit ip any any
```

Step 2 Create a class map to identify the traffic that should be diverted to the AIP SSM. Use the **class-map** command to do so, as follows:

```
hostname(config)# class-map class_map_name
hostname(config-cmap)#
```

where *class_map_name* is the name of the traffic class. When you enter the **class-map** command, the CLI enters class map configuration mode.

Step 3 With the access list you created in Step 1, use a **match access-list** command to identify the traffic to be scanned:

```
hostname(config-cmap)# match access-list acl-name
```

Step 4 Create a policy map or modify an existing policy map that you want to use to send traffic to the AIP SSM. To do so, use the **policy-map** command, as follows:

```
hostname(config-cmap)# policy-map policy_map_name
hostname(config-pmap)#
```

where *policy_map_name* is the name of the policy map. The CLI enters the policy map configuration mode and the prompt changes accordingly.

Step 5 Specify the class map, created in Step 2, that identifies the traffic to be scanned. Use the **class** command to do so, as follows:

```
hostname(config-pmap)# class class_map_name
hostname(config-pmap-c)#
```

where *class_map_name* is the name of the class map you created in Step 2. The CLI enters the policy map class configuration mode and the prompt changes accordingly.

Step 6 Assign the traffic identified by the class map as traffic to be sent to the AIP SSM. Use the **ips** command to do so, as follows:

```
hostname(config-pmap-c)# ips {inline | promiscuous} {fail-close |
fail-open}
```

The **inline** and **promiscuous** keywords control the operating mode of the AIP SSM. The **fail-close** and **fail-open** keywords control how the adaptive security appliance treats traffic when the AIP SSM is unavailable. For more information about the operating modes and failure behavior, see the "AIP SSM Configuration" section on page 9-1.

Step 7 Use the **service-policy** command to apply the policy map globally or to a specific interface, as follows:

```
hostname(config-pmap-c)# service-policy policy_map_name [global |
interface interface_ID]
hostname(config)#
```

where *policy_map_name* is the policy map you configured in Step 4. If you want to apply the policy map to traffic on all the interfaces, use the **global** keyword. If you want to apply the policy map to traffic on a specific interface, use the **interface** *interface_ID* option, where *interface_ID* is the name assigned to the interface with the **nameif** command.

Only one global policy is allowed. You can override the global policy on an interface by applying a service policy to that interface. You can only apply one policy map to each interface.

The adaptive security appliance begins diverting traffic to the AIP SSM as specified.

The following example diverts all IP traffic to the AIP SSM in promiscuous mode, and blocks all IP traffic should the AIP SSM card fail for any reason:

```
hostname(config)# access-list IPS permit ip any any
hostname(config)# class-map my-ips-class
hostname(config-cmap)# match access-list IPS
hostname(config-cmap)# policy-map my-ids-policy
hostname(config-pmap)# class my-ips-class
hostname(config-pmap-c)# ips promiscuous fail-close
hostname(config-pmap-c)# service-policy my-ips-policy global
```

Sessioning to the AIP SSM and Running Setup

After you have completed configuration of the ASA 5500 series adaptive security appliance to divert traffic to the AIP SSM, session to the AIP SSM and run the setup utility for initial configuration.

Note You can either session to the SSM from the adaptive security appliance (by using the **session 1** command) or you can connect directly to the SSM using SSH or Telnet on its management interface. Alternatively, you can use ASDM.

To session to the AIP SSM from the adaptive adaptive security appliance, perform the following steps:

Step 1 Enter the **session 1** command to session from the ASA 5500 series adaptive security appliance to the AIP SSM:

```
hostname# session 1
Opening command session with slot 1.
Connected to slot 1. Escape character sequence is 'CTRL-^X'.
```

Step 2 Enter the username and password. The default username and password are both **cisco**:

Note The first time you log in to the AIP SSM you are prompted to change the default password. Passwords must be at least eight characters long and *not* a dictionary word.

```
login: cisco
Password:
Last login: Fri Sep  2 06:21:20 from xxx.xxx.xxx.xxx
***NOTICE***
This product contains cryptographic features and is subject to United
States
and local country laws governing import, export, transfer and use.
Delivery
of Cisco cryptographic products does not imply third-party authority
to import,
export, distribute or use encryption. Importers, exporters,
distributors and
users are responsible for compliance with U.S. and local country laws.
By using
```

```
this product you agree to comply with applicable laws and regulations.
If you
are unable to comply with U.S. and local laws, return this product
immediately.

A summary of U.S. laws governing Cisco cryptographic products may be
found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email
to
export@cisco.com.

***LICENSE NOTICE***
There is no license key installed on the system.
Please go to http://www.cisco.com/go/license
to obtain a new license or install a license.
AIP SSM#
```

Note If you see the license notice above (which displays only is some versions of software), you can ignore the message until you need to upgrade the signature files on the AIP SSM. The AIP SSM continues to operate at the current signature level until a valid license key is installed. You can install the license key at a later time. The license key does not affect the current functionality of the AIP SSM.

Step 3 Enter the **setup** command to run the setup utility for initial configuration of the AIP SSM:

```
AIP SSM# setup
```

What to Do Next

You are now ready to configure the adaptive security appliance for intrusion prevention. Use the following documents to continue configuring the adaptive security appliance for your implementation.

To Do This ...	See ...
Configure the IPS sensor	*Configuring the Cisco Intrusion Prevention System Sensor Using the Command Line Interface* *Cisco Intrusion Prevention System Command Reference*
Optimize performance by creating more efficient service policies	"Managing AIP SSM and CSC SSM" in *Cisco Security Appliance Command Line Configuration Guide*

After you have configured the IPS sensory and AIP SSM software, you may want to consider performing some of the following additional steps:

To Do This ...	See ...
Refine configuration and configure optional and advanced features	*Cisco Security Appliance Command Line Configuration Guide*
Learn about daily operations	*Cisco Security Appliance Command Reference* *Cisco Security Appliance Logging Configuration and System Log Messages*
Review hardware maintenance and troubleshooting information	*Cisco ASA 5500 Series Hardware Installation Guide*

You can configure the adaptive security appliance for more than one application. The following sections provide configuration procedures for other common applications of the adaptive security appliance.

To Do This ...	See ...
Configure protection of a DMZ web server	Chapter 6, "Scenario: DMZ Configuration"
Configure a remote-access VPN	Chapter 7, "Scenario: Remote-Access VPN Configuration"
Configure a site-to-site VPN	Chapter 8, "Scenario: Site-to-Site VPN Configuration"

CHAPTER 10

Configuring the CSC SSM

The ASA 5500 series adaptive security appliance supports the CSC SSM, which runs Content Security and Control software. The CSC SSM provides protection against viruses, spyware, spam, and other unwanted traffic. It accomplishes this by scanning the FTP, HTTP, POP3, and SMTP traffic that is diverted to it by the adaptive security appliance.

Note The CSC SSM requires ASA software release 7.1.1 or later.

This chapter includes the following sections:

About the CSC SSM

The CSC SSM maintains a file containing signature profiles of suspicious content, updated regularly from an update server at Trend Micro. The CSC SSM scans traffic it receives from the adaptive security appliance and compares it to the content profiles it obtains from Trend Micro. It then forwards legitimate content on to the adaptive security appliance for routing, or blocks and reports content that is suspicious.

In addition to obtaining content profiles from Trend Micro, system administrators can also customize the configuration so that the CSC SSM scans for additional traffic types or locations. For example, system administrators can configure the CSC SSM to block or filter specific URLs, as well as scan for FTP and email parameters.

You use ASDM for system setup and monitoring of the CSC SSM. For advanced configuration of content security policies in the CSC SSM software, you access the web-based GUI for the CSC SSM by clicking links within ASDM.

This chapter describes how to configure the adaptive security appliance for the deployment. Use of the CSC SSM GUI is explained in the *Cisco Content Security and Control SSM Administrator Guide*.

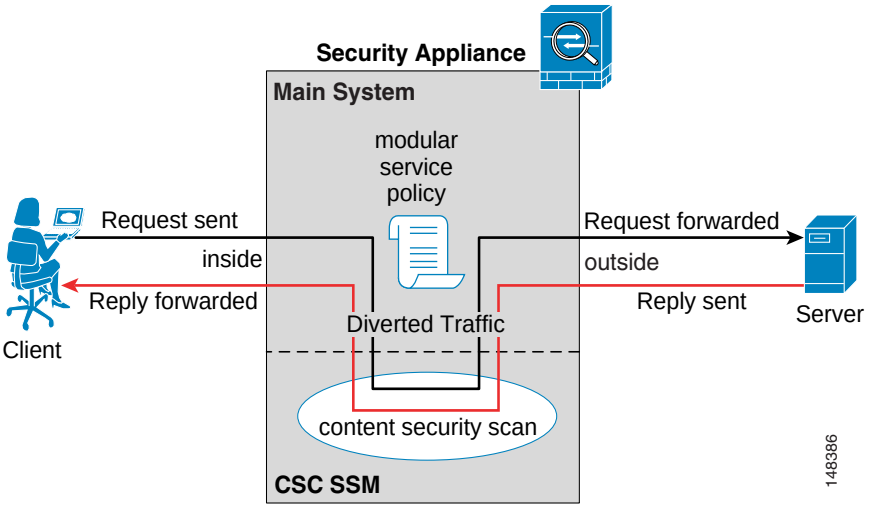
About Deploying the Security Appliance with the CSC SSM

In a network in which the adaptive security appliance is deployed with the CSC SSM, you configure the adaptive security appliance to send to the CSC SSM only the types of traffic that you want to be scanned.

Figure 10-1 illustrates the basic traffic flow between a company network, the adaptive security appliance and CSC SSM, and the Internet. The network illustrated in Figure 10-1 includes the following:

- An adaptive security appliance with a CSC SSM installed and configured
- A service policy on the adaptive security appliance specifies which traffic is diverted to the CSC SSM for scanning

Figure 10-1 CSC SSM Traffic Flow



In this example, clients could be network users who are accessing a website, downloading files from an FTP server, or retrieving mail from a POP3 server.

In this configuration, the traffic flow is as follows:

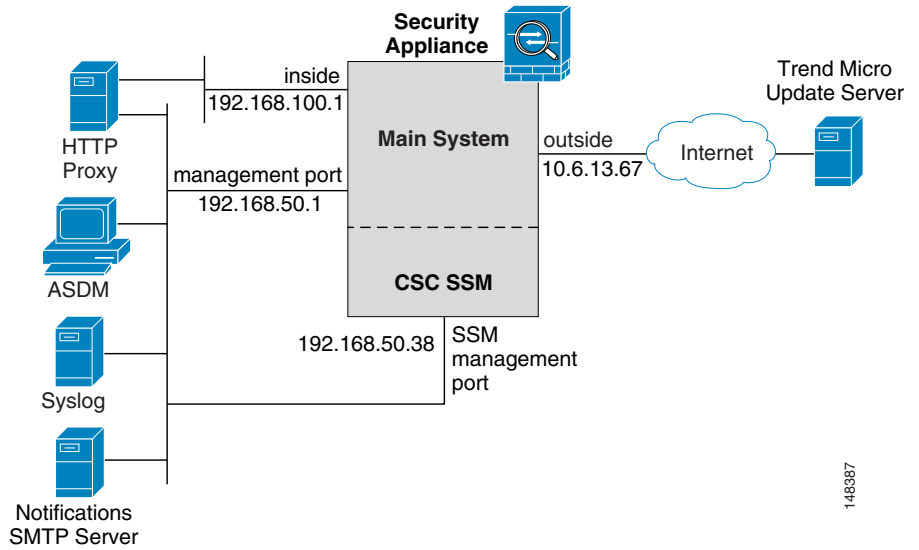
1. The client initiates a request.
2. The adaptive security appliance receives the request and forwards it to the Internet.
3. When the requested content is retrieved, the adaptive security appliance determines whether its service policies define this content type as one that should be diverted to the CSC SSM for scanning, and does so if appropriate.
4. The CSC SSM receives the content from the adaptive security appliance, scans it and compares it to its latest update of the Trend Micro content filters.
5. If the content is suspicious, the CSC SSM blocks the content and reports the event. If the content is not suspicious, the CSC SSM forwards the requested content back to the adaptive security appliance for routing.

Note The CSC SSM handles SMTP traffic somewhat differently than other content types. After the CSC SSM receives SMTP traffic and scans it, it does not forward the traffic back to the adaptive security appliance for routing. Rather, the CSC SSM forwards the SMTP traffic directly to the SMTP servers protected by the adaptive security appliance.

Scenario: Security Appliance with CSC SSM Deployed for Content Security

Figure 10-2 is an illustration of a typical deployment of the adaptive security appliance with CSC SSM. Properties of this scenario are used as examples in the configuration procedures later in this chapter.

Figure 10-2 CSC SSM Deployment Scenario



In this scenario, the customer has deployed an adaptive security appliance with a CSC SSM for content security. Of particular interest are the following points:

- The adaptive security appliance is on a dedicated management network. Although using a dedicated management network is not required, we recommend it for security purposes.
- This adaptive security appliance configuration has two management ports: one for the adaptive security appliance itself, and another for the CSC SSM. All administration hosts must be able to access both IP addresses.
- The HTTP proxy server is connected to both the inside network and the dedicated management network. This enables the CSC SSM to retrieve updated content security filters from the Trend Micro update server.
- The management network includes an SMTP server so that administrators can be notified of CSC SSM events. The management network also includes a syslog server to store logs generated by the CSC SSM.

Configuration Requirements

When you plan the adaptive security appliance deployment, it is critical that the network adheres to the following requirements:

- The SSM management port IP address must be accessible by the hosts used to run ASDM. However, the IP addresses for the SSM management port and the adaptive security appliance management interface can be in different subnets.
- The SSM management port must be able to connect to the Internet so that the CSC SSM can reach the Trend Micro update server.

Configuring the CSC SSM for Content Security

If you ordered your adaptive security appliance with the optional CSC SSM module, there are several steps you need to perform to complete the initial configuration. Some configuration steps are performed on the adaptive security appliance, and some steps are performed in the software running on the CSC SSM.

If you followed the procedures in earlier chapters of this document, at this point you have an ASA system running with licensed software, and you have entered basic system values using the setup Wizard. Your next steps are to configure the adaptive security appliance for a content security deployment.

The basic steps are:

1. Obtain software activation key from Cisco.com.
2. Gather the information you need to configure the CSC SSM.
3. Obtain activation keys from cisco.com.
4. Open ASDM, which is used for all configuration tasks in this setup process.
5. Verify time settings.
6. Run the CSC setup wizard to configure the CSC SSM.
7. Configure the adaptive security appliance to divert traffic to the CSC SSM for scanning.

These steps are described in detail in the sections that follow.

Obtain Software Activation Key from Cisco.com

With the CSC SSM, you should have received a Product Authorization Key (PAK). Use the PAK to register the CSC SSM at the following URL:

`http://www.cisco.com/go/license`

After you register, you will receive activation keys by email. The activation keys are required before you can complete the procedure described in the "Run the CSC Setup Wizard" section on page 10-9.

Gather Information

Before you start configuring the adaptive security appliance and the CSC SSM, gather the following information:

IP address netmask for the CSC SSM management port, gateway IP address and netmask. (The adaptive security appliance IP address was assigned when you performed the Setup Wizard, described in Chapter 5, "Configuring the Adaptive Security Appliance."

Note The SSM management port IP address must be accessible by the hosts used to run ASDM. The IP addresses for the SSM management port and the adaptive security appliance management interface can be in different subnets.

- Hostname and domain name to be used for the CSC SSM
- DNS Server IP address
- HTTP proxy server IP address (if your network uses a proxy for HTTP access to the Internet)
- Email address to be used for email notifications; IP address and port number of an SMTP server
- IP addresses of hosts and networks to be allowed management access to the CSC SSM

Launch ASDM

You use ASDM to configure and manage the CSC SSM. For advanced configuration of content security policies in the CSC SSM software, you access the web-based GUI for the CSC SSM by clicking links within ASDM.

To launch ASDM, perform the following steps:

Step 1 On a PC that has access to the management ports for the adaptive security appliance and the CSC SSM, launch an Internet browser.

Step 2 In the address field of the browser, enter this URL: **https://*IP_address/***

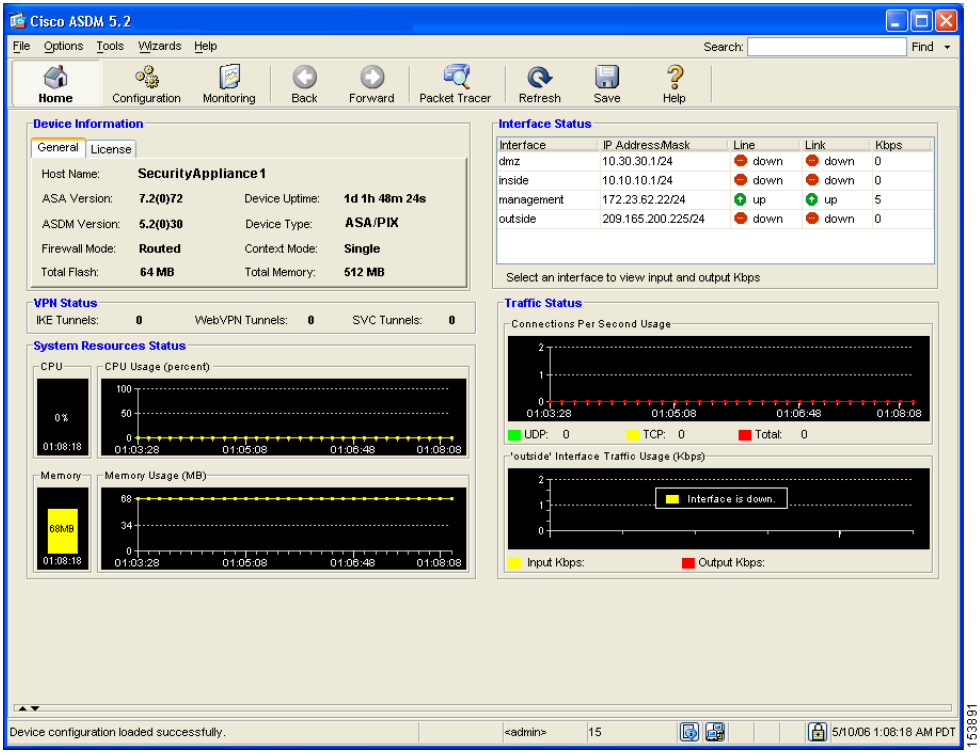
where *IP_address* is the IP address of the adaptive security appliance.

Note The adaptive security appliance ships with a default IP address of 192.168.1.1. Remember to add the "**s**" in "**https**" or the connection fails. HTTPS (HTTP over SSL) provides a secure connection between your browser and the adaptive security appliance.

Step 3 In the dialog box that requires a username and password, leave both fields empty. Press **Enter**.

Step 4 Click **Yes** to accept the certificates. Click **Yes** for all subsequent authentication and certificate dialog boxes.

The ASDM Main window appears.



Verify Time Settings

Verify the accuracy of the adaptive security appliance time settings, including the time zone. Time accuracy is important for logging security events, automatic updates of the content filter lists on the CSC SSM. It is also important for licensing, as licenses are time sensitive.

- If you control time settings manually, verify the clock settings. In ASDM, click **Configuration > Properties > Device Administration > Clock**.

- If you are using NTP to control time settings, verify the NTP configuration. In ASDM, click **Configuration > Properties > Device Administration > NTP**.

Run the CSC Setup Wizard

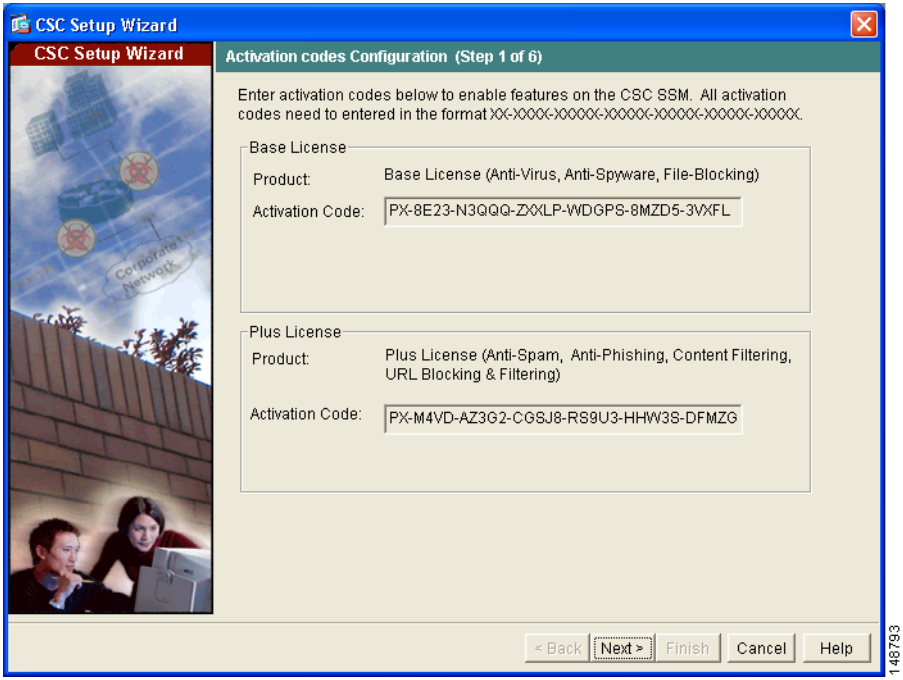
Step 1 In the main ASDM window, click the **Configuration** tab.

Step 2 In the left pane, click the **Trend Micro Content Security** tab.

The Wizard Setup screen appears.

Step 3 In Step 1 of the CSC Wizard, enter the **Software Activation Codes** for the Base License and, optionally, the activation code for the Plus License.

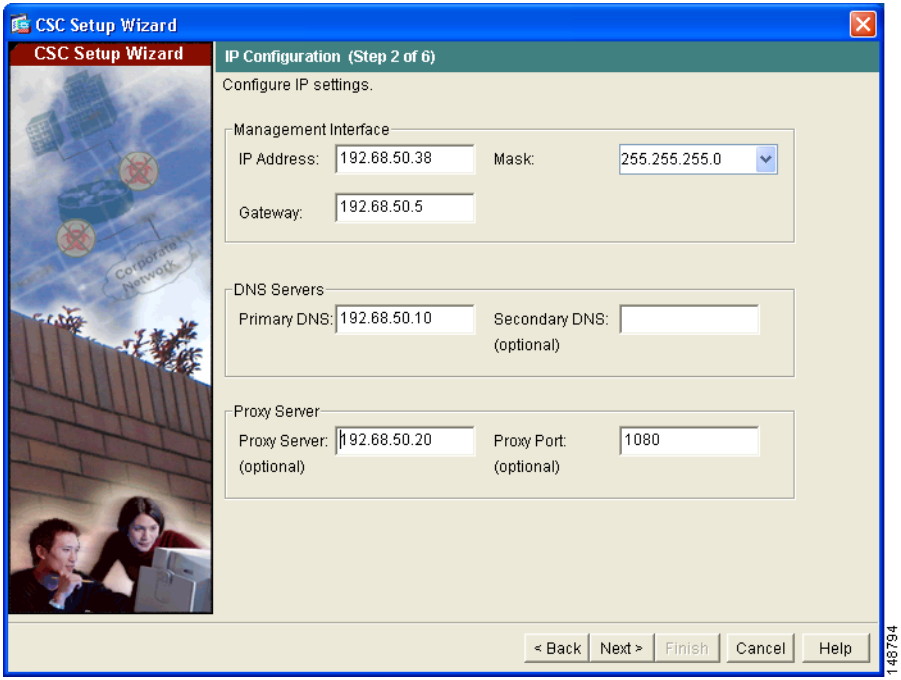
You can enter the activation code for the Plus license after the initial configuration of the CSC SSM.



Step 4 Click **Next**.

Step 5 In Step 2 of the CSC Wizard, enter the following information:

- IP address, netmask and gateway IP address for the CSC Management interface
- IP address for the Primary DNS server
- IP address and proxy port of the HTTP proxy server (only if your network uses an HTTP proxy for sending HTTP requests to the Internet)



Step 6 Click **Next**.

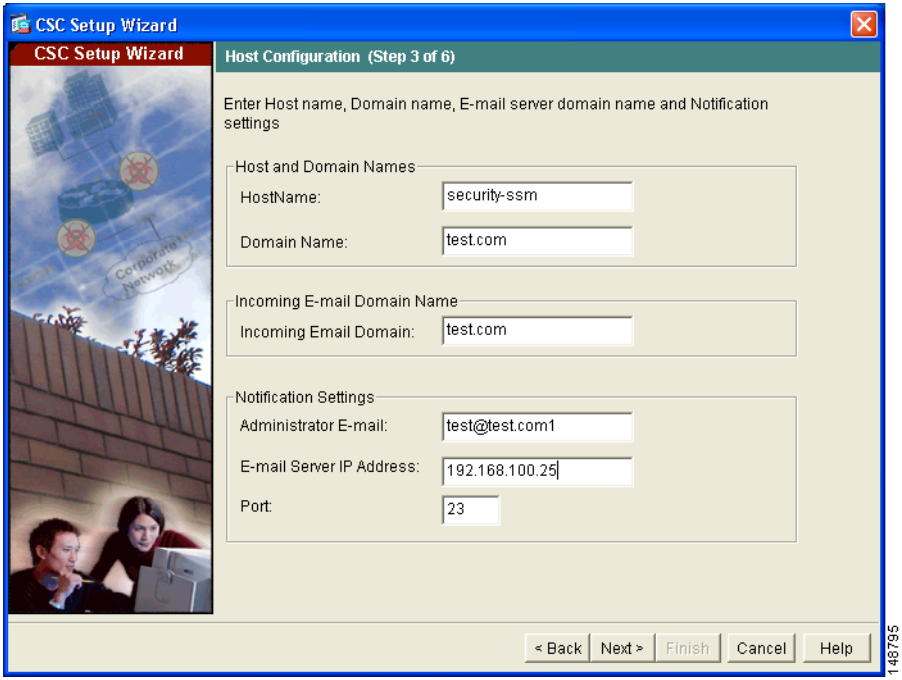
Step 7 In Step 3 of the CSC Setup Wizard, enter the following information:

- **Hostname** and **Domain** name of the CSC SSM.

- **Domain** name used by the local mail server as the incoming domain.

Note Anti-SPAM policies are applied only to email traffic coming into this domain.

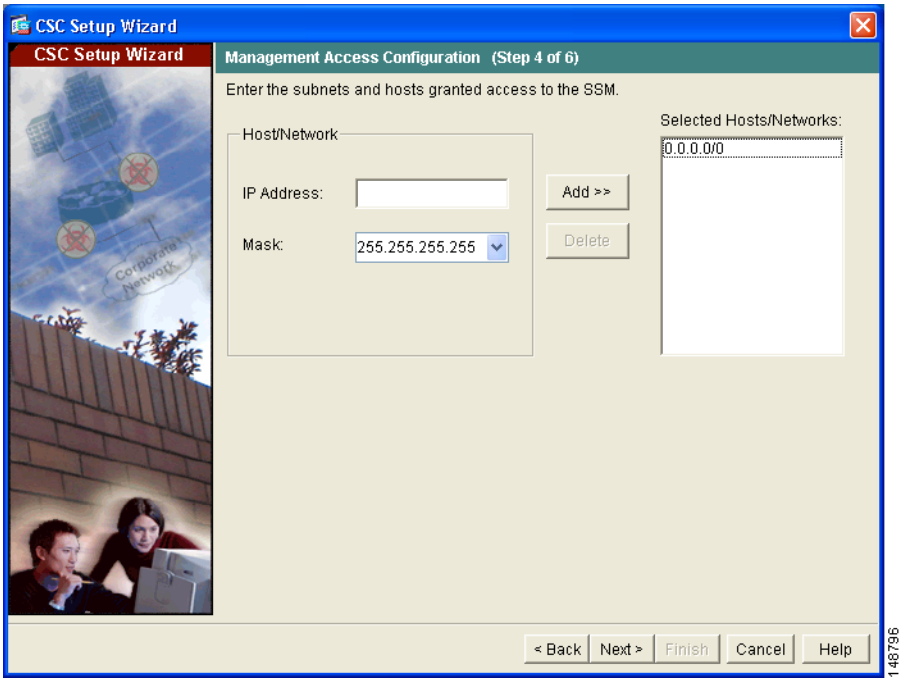
- Administrator email address and the email server IP address and port to be used for notifications.



Step 8 Click **Next**.

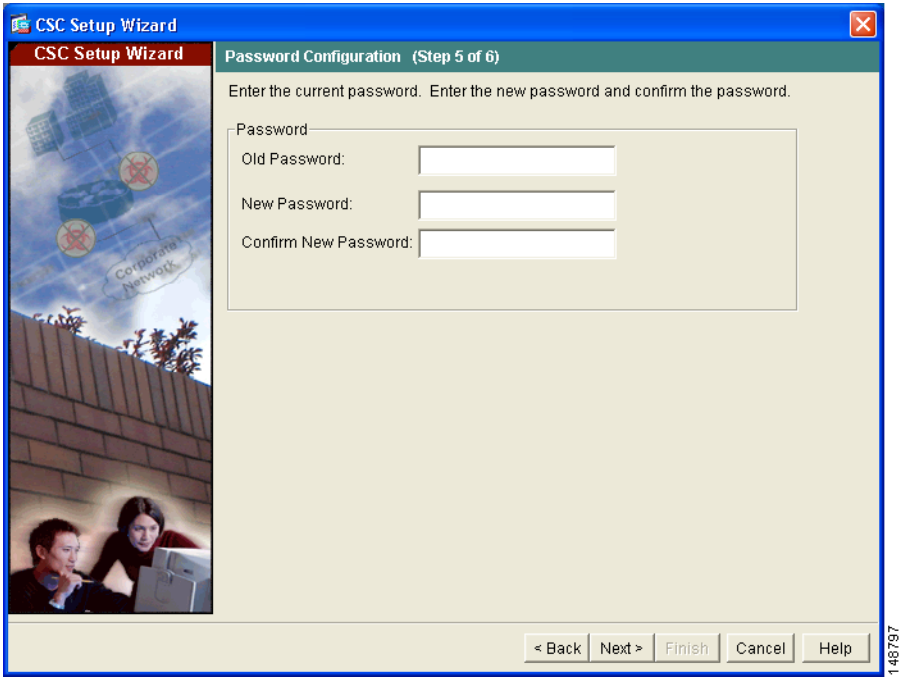
Step 9 In Step 4 of the CSC Setup Wizard, enter the IP address and mask for each subnet and host that should have management access to the CSC SSM.

By default, all networks have management access to the CSC SSM. For security purposes, we recommend that you restrict access to specific subnets or management hosts.



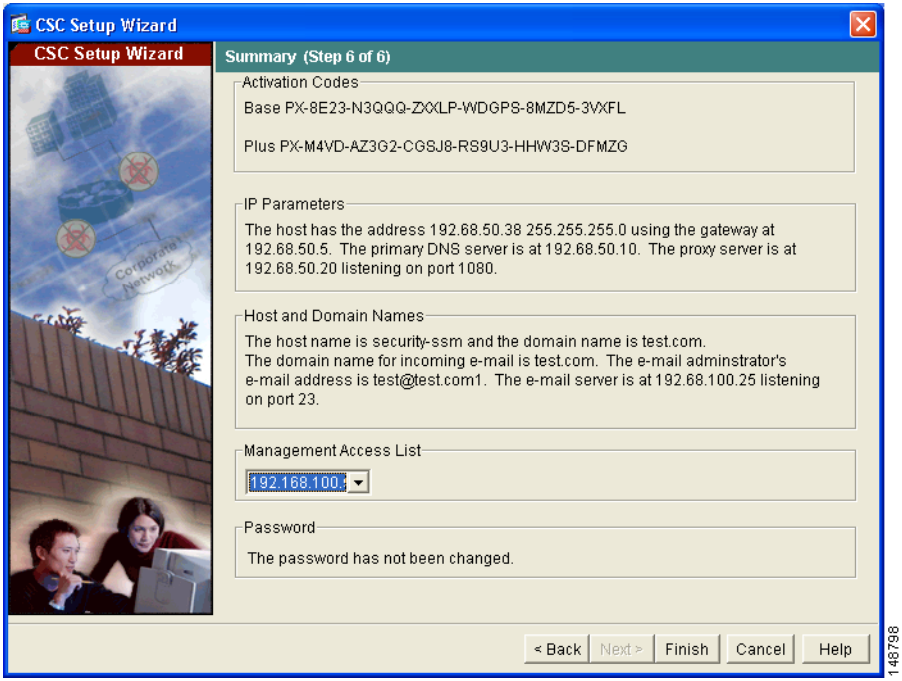
Step 10 Click **Next**.

Step 11 In Step 5 of the CSC Setup Wizard, enter a new password for management access. Enter the factory default password, "cisco," in the Old Password field.



Step 12 Click **Next**.

Step 13 In Step 6 of the CSC Setup Wizard, review configuration settings you just entered for the CSC SSM.



If you are satisfied with these settings, click **Finish**.

ASDM shows a message indicating that the CSC device is now active.

Divert Traffic to the CSC SSM for Content Scanning

The adaptive security appliance diverts packets to the CSC SSM after firewall policies are applied but before the packets exit the egress interface. For example, packets that are blocked by an access list are not forwarded to the CSC SSM.

Configure service policies to specify which traffic the adaptive security appliance should divert to the CSC SSM. The CSC SSM can scan HTTP, POP3, FTP, and SMTP traffic sent to the well-known ports for those protocols.

To simplify the initial configuration process, this procedure creates a global service policy that diverts all traffic for the supported protocols to the CSC SSM, both inbound and outbound. Because scanning all traffic coming through the adaptive security appliance may reduce the performance of the adaptive security appliance and the CSC SSM, you may want to revise this security policy later. For example, it is not usually necessary to scan all traffic coming from your inside network because it is coming from a trusted source. By refining the service policies so that the CSC SSM scans only traffic from untrusted sources, you can achieve your security goals and maximize performance of the adaptive security appliance and the CSC SSM.

To create a global service policy that identifies traffic to be scanned, perform the following steps:

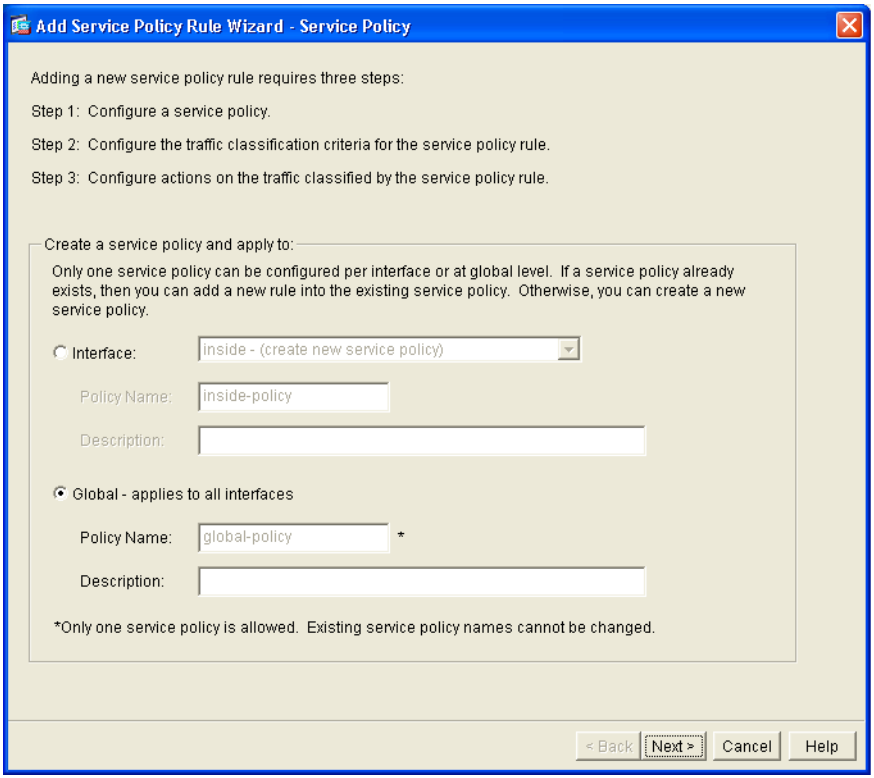
Step 1 In the main ASDM window, click the **Configuration** tab.

Step 2 Click **Security Policies**, and then click the **Service Policy Rules** radio button.

Step 3 Click **Add**.

The Add Service Policy Rule appears.

Step 4 In the Service Policy page, click the **Global - applies to all interfaces** radio button.

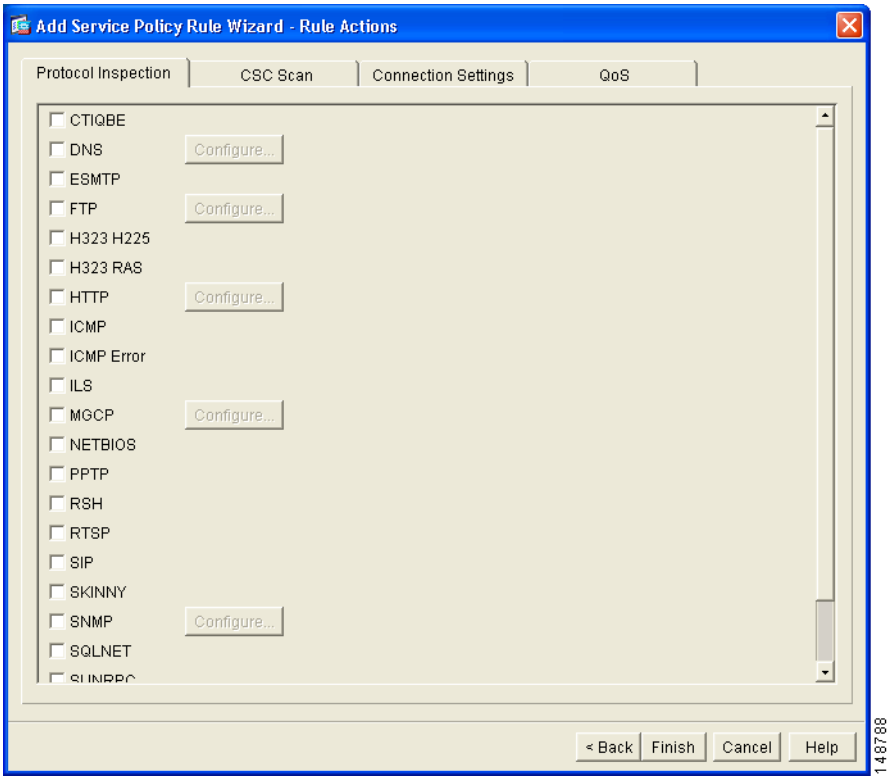


Step 5 Click **Next.** The Traffic Classification Criteria page appears.

Step 6 In the Traffic Classification Criteria page, click the **User class-default as the traffic class** radio button.

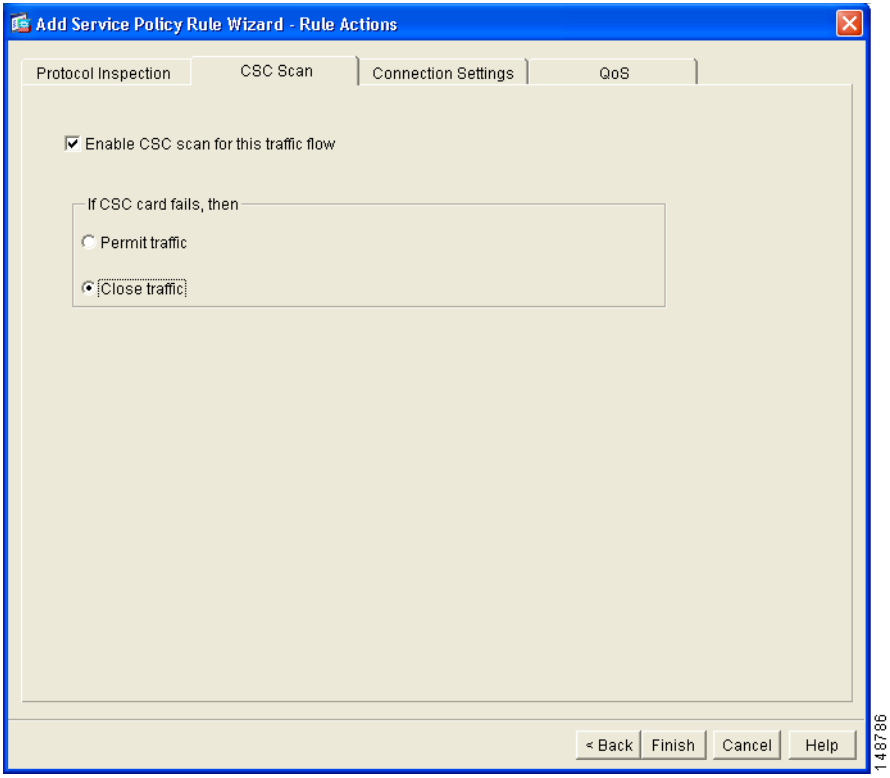
Step 7 Click **Next**. The Add Service Policy Rule Wizard - Rule Actions page appears.

Step 8 In the Service Policy Rule Wizard, click the **CSC Scan** tab.



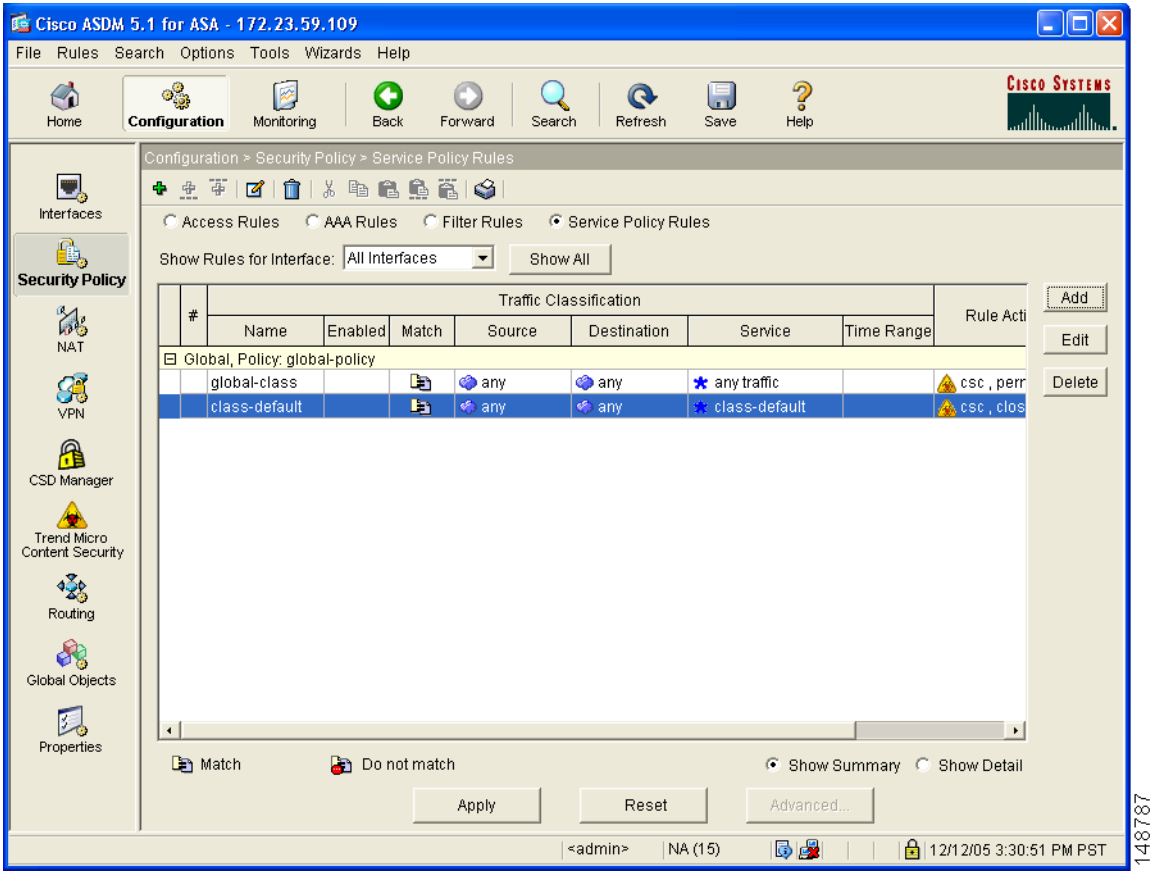
Step 9 On the CSC Scan tab page, check the **Enable CSC scan for this traffic flow** check box.

In the **If CSC card fails, then** area, choose whether the adaptive security appliance should permit or deny selected traffic if the CSC SSM is unavailable.



Step 10 Click **Finish**.

The new service policy appears in the Service Policy Rules pane.



Step 11 Click **Apply**.

By default, the CSC SSM is configured to perform content security scans enabled by the license you purchased (which may include anti-virus, anti-spam, anti-phishing, and content filtering). It is also configured to get periodic updates from the Trend Micro update server.

If included in the license you purchased, you can create custom settings for URL blocking and URL filtering, as well as email and FTP parameters. For more information, see the *Cisco Content Security and Control SSM Administrator Guide*.

What to Do Next

You are now ready to configure the Trend Micro Interscan for Cisco CSC SSM software. Use the following documents to continue configuring the adaptive security appliance for your implementation.

To Do This ...	See ...
Configure CSC SSM software, such as advanced security policies	*Cisco Content Security and Control SSM Administrator Guide*
Configure additional CSC SSM features in ASDM, including content filtering	ASDM online help (click the **Configuration** or **Monitoring** tab, then click the **Trend Micro Content Security** tab)
Optimize performance by creating more efficient service policies	"Managing AIP SSM and CSC SSM" in *Cisco Security Appliance Command Line Configuration Guide*

After you have configured the CSC SSM software, you may want to consider performing some of the following additional steps:

To Do This ...	See ...
Refine configuration and configure optional and advanced features	*Cisco Security Appliance Command Line Configuration Guide*
Learn about daily operations	*Cisco Security Appliance Command Reference* *Cisco Security Appliance Logging Configuration and System Log Messages*
Review hardware maintenance and troubleshooting information	*Cisco ASA 5500 Series Hardware Installation Guide*

You can configure the adaptive security appliance for more than one application. The following sections provide configuration procedures for other common applications of the adaptive security appliance.

To Do This ...	See ...
Configure protection of a DMZ web server	Chapter 6, "Scenario: DMZ Configuration"
Configure a remote-access VPN	Chapter 7, "Scenario: Remote-Access VPN Configuration"
Configure a site-to-site VPN	Chapter 8, "Scenario: Site-to-Site VPN Configuration"

Configuring the 4GE SSM for Fiber

The 4GE Security Services Module (SSM) has four Ethernet ports, and each port has two media type options: SFP (Small Form-Factor Pluggable) fiber or RJ 35. You can mix the copper and fiber ports using the same 4GE card.

Note The 4GE SSM requires ASA software release 7.04 or later.

This chapter includes the following sections:

Note Because the default media type setting is Ethernet, you do not need to change the media type setting for any Ethernet interfaces you use.

Cabling 4GE SSM Interfaces

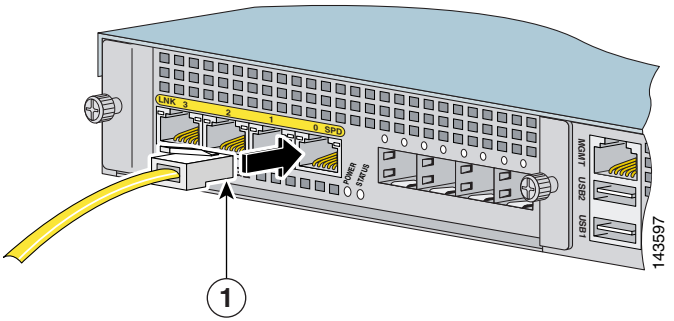
To cable 4GE SSM interfaces, perform the following steps for each port you want to connect to a network device:

Step 1 To connect an RJ-45 (Ethernet) interface to a network device, perform the following steps for each interface:

a. Locate a yellow Ethernet cable from the accessory kit.

b. Connect one end of the cable to an Ethernet port on the 4GE SSM as shown in Figure 11-1.

Figure 11-1 Connecting the Ethernet port



1	RJ-45 (Ethernet) port

c. Connect the other end of the cable to your network device.

Step 2 (Optional) If you want to use an SFP (fiber optic) port, install and cable the SFP modules as shown in Figure 11-2:

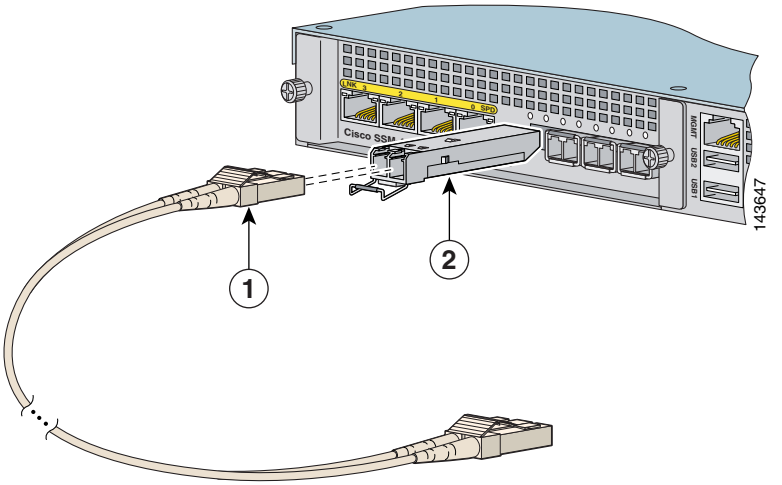
a. Insert and slide the SFP module into the SFP port until you hear a click. The click indicates that the SFP module is locked into the port.

b. Remove the optical port plugs from the installed SFP.

c. Locate the LC connector (fiber optic cable) in the 4GE SSM accessory kit.

d. Connect the LC connector to the SFP port.

Figure 11-2 Connecting the LC Connector



1	LC connector	**2**	SFP module

e. Connect the other end of the LC connector to your network device.

After you have attached any SFP ports to your network devices, you must also change the media type setting for each SFP interface. Continue with the following procedure, "Setting the 4GE SSM Media Type for Fiber Interfaces (Optional)."

Setting the 4GE SSM Media Type for Fiber Interfaces (Optional)

If you are using fiber interfaces, for each SFP interface you must change the media type setting from the default setting (Ethernet) to Fiber Connector.

Note Because the default media type setting is Ethernet, you do not need to change the media type setting for Ethernet interfaces you use.

To set the media type for SFP interfaces using ASDM, perform the following steps starting from the main ASDM window:

Step 1 At the top of the ASDM window, click the **Configuration** tab.

Step 2 On the left side of the ASDM window, click the **Interfaces** tab.

Step 3 Click the **4GE SSM** interface and click **Edit**. The Edit Interface dialog box appears.

Step 4 Click **Configure Hardware Properties**. The Hardware Properties dialog box appears.

Step 5 From the Media Type drop-down list, choose **Fiber Connector**.

Step 6 Click **OK** to return to the Edit Interfaces dialog box, then click **OK** to return to the interfaces configuration dialog box.

Step 7 Repeat this procedure for each SFP interface.

You can also set the media type from the command line. For more information, see "Configuring Ethernet Settings and Subinterfaces" in the *Cisco Security Appliance Command Line Configuration Guide*.

What to Do Next

You have completed the initial configuration. You may want to consider performing some of the following additional steps:

To Do This ...	See ...
Refine configuration and configure optional and advanced features	*Cisco Security Appliance Command Line Configuration Guide*
Learn about daily operations	*Cisco Security Appliance Command Reference* *Cisco Security Appliance Logging Configuration and System Log Messages*
Review hardware maintenance and troubleshooting information	*Cisco ASA 5500 Series Hardware Installation Guide*

Obtaining a DES License or a 3DES-AES License

Cisco adaptive security appliances are available either with a DES or 3DES-ASE license that provides encryption technology to enable specific features, such as secure remote management (SSH, ASDM, and so on), site-to-site VPN, and remote access VPN. The license is enabled through an encryption license key.

If you ordered your adaptive security appliance with a DES or 3DES-AES license, the encryption license key comes with the adaptive security appliance.

If you are a registered user of Cisco.com and would like to obtain a 3DES/AES encryption license, go to the following website:

http://www.cisco.com/go/license

If you are not a registered user of Cisco.com, go to the following website:

https://tools.cisco.com/SWIFT/Licensing/RegistrationServlet

Provide your name, e-mail address, and the serial number for the adaptive security appliance as it appears in the show version command output.

Note You will receive the new activation key for your adaptive security appliance within two hours of requesting the license upgrade.

For more information on activation key examples or upgrading software, see the *Cisco Security Appliance Command Line Configuration Guide*.

To use the activation key, perform the following steps:

	Command	Purpose
Step 1	`hostname# show version`	Shows the software release, hardware configuration, license key, and related uptime data.
Step 2	`hostname# configure terminal`	Enters global configuration mode.
Step 3	`hostname(config)# activation-key` *activation-5-tuple-key*	Updates the encryption activation key by replacing the *activation-4-tuple-key* variable with the activation key obtained with your new license. The *activation-5-tuple-key* variable is a five-element hexadecimal string with one space between each element. An example is 0xe02888da 0x4ba7bed6 0xf1c123ae 0xffd8624e. The "0x" is optional; all values are assumed to be hexadecimal.
Step 4	`hostname(config)# exit`	Exits global configuration mode.
Step 5	`hostname# copy running-config startup-config`	Saves the configuration.
Step 6	`hostname# reload`	Reboots the adaptive security appliance and reloads the configuration.